



**PRIMUS
PARTNERS[®]**

Solutions for Tomorrow



Draft Digital Personal Data Protection Rules 2025

Primus Summary

Draft Digital Personal Data Protection Rules, 2025

January 2025

The document is a summary of the Digital Personal Data Protection (DPDP) Rules 2025 which have emanated from the DPDP Act 2023. The Rules detail out requisite clauses of the Act, including seeking consent, further obligations of the Consent Manager, what and what not in case of a data breach, storage and processing of data, processing of children data, functions of the Data Protection Board, Appeal process, among other details. The Rules aim to change the data management process of the country while also reinstating the philosophy of user vis-à-vis Data Principal protection. These Rules will be applicable to digital intermediaries, user facing platforms, apps and websites, cloud service providers and all data collecting or managing entities. Feedback can be submitted by 18 February 2025.

Note: The note does not necessarily carry the clauses and points that have already been mentioned in the original DPDP Act or those which stem from the IT Act and its Rules.



1

Key Definitions

The Rules does not introduce many new concepts. However, there are few definitions and meanings which are noteworthy, including refurbishment of concepts previously established in the IT Act.

- ❖ **User account:** An online account created by a Data Principal with a Data Fiduciary. It includes profiles, pages, handles, or any similar features that allow the Data Principal to use the services provided by the Data Fiduciary.
- ❖ **Digital Locker Service Provider:** Digital Locker service provider means an intermediary including a body corporate or an agency of the appropriate Government, as may be notified by the Government, to provide Digital Locker, access gateways and, or, repository facilities electronically, in accordance with the rules made under the Information Technology Act 2000.
- ❖ **Identifier:** 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.
- ❖ **Computer Resource (as assigned in the IT Act 2000):** means computer, computer system, computer network, data, computer data base or software.



Revisiting Essential Concepts of DPDP Act 2023

Data Fiduciary: A person or entity that decides how personal data is processed, including the purpose and methods. This can be a social media company, a financial institution, MSMEs, etc.

Data Principal: A person whose personal data is being processed by a data fiduciary. In principle, it is the individual who owns the data and has the right to control how it is used.

2

Seeking Consent of Data Principal

Every Request for Consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal.

The notice shall have the following characteristics -

- ❖ Clarity and Independence: Notices must be clear, and written in plain language. And presented independently of other information, ensuring they are not bundled with other information.
- ❖ Content Requirements: Include an **itemized description** of personal data collected, its purpose, and the goods/services enabled by processing.
- ❖ Consent Management: Provide direct links for withdrawing consent, exercising rights (such as the right to access, correction, or deletion of personal data), and filing complaints with the Board.
- ❖ User Accessibility: Ensure notices are accessible, user-friendly, and inclusive for individuals with disabilities.

3

Processing for a Subsidy, Benefit, Service by the State

The State and its instrumentalities may process personal data to provide subsidies, benefits, services, certificates, licenses, or permits under law, policy, or using public funds.

- ❖ Standards for Processing (as per Schedule 2):
- ❖ Processing must be lawful, limited to necessary data, and aimed at specified purposes.
- ❖ Accuracy of data should be ensured, with reasonable security safeguards to prevent breaches.
- ❖ Data must be retained only as long as necessary for its purpose or as mandated by law.
- ❖ Provide clear intimation to Data Principals, including contact information and rights under the Act.



4

Obligations of a Consent Manager

The DPDP Act 2023 had introduced the concept of Consent Manager, who is an entity registered with the Data Protection Board and who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent, and interoperable platform.

While specifics of contractual agreements remain to be detailed out, the Rules do further out more on Consent Managers –

A Consent Manager, **to be registered with the Board, must fulfil several conditions as per the new DPDP Rules.** To summarise, they need to be a domestically incorporated company with a net worth of at least two crore rupees. They should have sufficient capacity, including technical, operational and financial capacity, with the leadership having a record of fairness and integrity. The Consent Manager must always act in the best interest of the Data Principal, avoiding any conflicts of interest with Data Fiduciaries. They have adequate technical and organizational measures in place to ensure adherence to specific data protection standards as set by the Board from time to time.

Once registered, the Consent Manager has numerous obligations. They must establish a secure, transparent platform that allows Data Principals to manage their consent and data sharing with the Data Fiduciary without the Consent Manager accessing the personal data. They are also responsible for keeping digital records of consent requests and data sharing activities for a minimum of seven years and providing Data Principals with access to these records. Consent Managers must also publish, in an accessible manner, details about their key management, major shareholders (holding over 2% equity), and corporate entities linked to their promoters or management. Additional disclosures may be mandated by the Board for transparency. The Consent Manager shall not sub-contract or assign the performance to another entity of any of its obligations under the Act and these rules. Additionally, they are required to maintain a website or app as the primary means for Data Principals to access their services, ensure robust security measures to prevent data breaches, and have effective audit mechanisms in place. The Board retains the right to suspend or cancel the registration of a Consent Manager, after providing them an opportunity of being heard, if they fail to adhere to these conditions or obligations.

5

Intimation of Personal Data Breach

When a Data Fiduciary becomes aware of a personal data breach, they are required to –

- ❖ Promptly inform the Board a comprehensive description of the breach. This includes the nature of the breach, when and for how long it occurred, its location, the extent and type of data involved, the potential impact.
- ❖ Within 72 hours of becoming aware of the breach, the Data Fiduciary must further detail the events and reasons leading to the breach, the extent and number of Data Principals affected, any updates on previous intimations, actions taken or proposed to mitigate risks, findings about the person responsible for the breach, and remedial measures to prevent future occurrences.

Additionally,

- ❖ The Data Fiduciary must inform affected Data Principals about the breach in a clear and concise manner. This communication should describe the breach, its timing and extent, potential consequences for the Data Principal, mitigation measures taken, recommended safety measures for the Data Principal, and contact details (a designated Data Protection Officer in case of a Significant Data Fiduciary) for further inquiries.
- ❖ This intimation should be made through the user account or a registered mode of communication.
- ❖ Also, the Board may grant extensions for these notifications upon written request from the Data Fiduciary, provided there are valid grounds for doing so.



6

Time Period for Specified Purpose to Be Deemed as No Longer Being Served

The DPDP Act 2023 states that a Data Fiduciary shall, unless retention is necessary for compliance with any law, erase personal data after the Data Principal withdraws her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served. The “purpose” here is deemed as no longer served, if the Data Principal either does not approach the Data Fiduciary for the performance of the specified purpose, or exercise any of her rights in relation to such processing.

❖ The new Rules have henceforth laid out the time period of **3 years from the date on which the Data principal last approached the Fiduciary or entity for performance of the specified purpose or exercise of her rights, or 3 years from the commencement of DPDP Rules 2023, whichever is latest.**

❖ The following class of intermediaries have been identified, and which **has two crore or more users (50 lakh in case of online gaming)** in India –

E-Commerce entity
Online Gaming intermediary
Social Media intermediary

- ❖ The Rules also detail out the “Purpose” as those other than - the enablement of the Data Principal to access her user account, her money accessible through any service provided or made available by the intermediary, and any virtual token or other similar thing acquired by her which is usable by her to avail any service.
- ❖ A Data Fiduciary must inform the Data Principal at least 48 hours before the scheduled erasure of their personal data, as per the applicable erasure timeline. This notice will state that the personal data will be erased due to the Data Principal's lack of contact for the “specified purpose”. However, the erasure will not occur if the Data Principal logs into their user account or initiates contact before the deadline.
- ❖ The above notification must be delivered through a registered communication mode or user account.

7

Critical Avenues – Child data; and data for Research

Processing of Children Data

When obtaining consent for processing a child’s personal data, a Data Fiduciary must diligently verify that the consenting individual is indeed the child's parent and not the child themselves.

- ❖ This verification can be achieved by referring to reliable identity and age details already available with the Data Fiduciary or collected with the individual's consent.
- ❖ Alternatively, it can be done using an electronic token linked to the individual's identity and age details. This token should be generated by an authorized entity, such as one appointed by the government or a Digital Locker service provider, ensuring legal compliance and authenticity.

Exemptions

Schedule IV of the new Rules outline conditions under which various classes of Data Fiduciaries are exempt from certain data processing restrictions for children. These classes include those entrusted by law to act in a child's interest, state instrumentalities providing certain services, clinical and mental health establishments, healthcare professionals, allied healthcare professionals, educational institutions, and individuals responsible for children in crèches or day care centers. The exemptions are primarily for purposes like health service provision, educational activity monitoring, child safety, and transportation safety.

Exemption for Research and Statistical Purposes

The Act exempts the processing of personal data for research, archiving, and statistical purposes, provided it doesn't involve decisions specific to a Data Principal.

- ❖ This exemption is conditional on maintaining reasonable security safeguards to prevent personal data breaches, purpose limitation, maintaining accuracy, and other conditions as mentioned in the Second Schedule of the Rules.
- ❖ The exemption for Research and statistical purpose ensures that necessary data processing for academic and policy research can occur while maintaining certain safeguards and standards to protect personal data.

Global Cues

UK’S GDPR provisions that an adult with parental responsibility must provide consent for processing if the child is under 13. This is a relaxed form of EU’s GDPR version, where the age limit is 16 years, the latter being close to India’s rules. Similarly, USA’s Children's Online Privacy Protection Act (COPPA) caps the age of parental control at 13, thus also showcasing EU’s relatively stricter norms over “data controllers”.

Concerns remain in India for certain industries/sectors like edtech, online gaming, etc.

8

Quick Catch

Some quick takeaways from what the rules tells us about a designated point of contact (POC) in fiduciaries, additional compliances for bigger entities, and user rights

POC for Data Principals

Data Fiduciaries are required to make available the business contact information of a designated person who can answer queries about personal data processing. This information should be prominently displayed on their website or app and communicated to Data Principals through all correspondence. For Significant Data Fiduciaries, this contact information must specifically be that of a **designated Data Protection Officer (DPO)**.

Additional Obligations for Significant Data Fiduciaries (SDFs)

Apart from assigning a DPO, SDFs are required to ensure that –

- ❖ **Annual Assessments and Audits:** An SDF must conduct a Data Protection Impact Assessment (DPIA) and an audit every 12 months from the date it is designated or included as such.
- ❖ **Submission of Key Findings:** The person conducting the DPIA and audit must submit a report to the Data Protection Board, detailing significant observations and findings.
- ❖ **Algorithmic Due Diligence:** The SDF must exercise due diligence to ensure that any algorithmic software it uses does not pose a risk to the rights of Data Principals.
- ❖ **Data Localization Requirements:** The SDF must ensure that personal data and traffic data specified by the Central Government, based on committee recommendations, are processed in India and not transferred outside the country.

Rights of Data Principals

The DPDP Rules also specify details on the rights of the Data Principal.

- ✓ Data Fiduciaries and Consent Managers must publish information enabling Data Principals to exercise their rights. This includes methods to request execution of the rights, identification particulars of the user required to access their data, details to locate previously given consent.
- ✓ This information should be easily accessible on the Fiduciary’s app or website or both.
- ✓ Data Principals can exercise their rights using these methods, for corrections, erasures, grievance redressals, or nominations they seek.
- ✓ Moreover, upon receiving a grievance, the Data Fiduciary or Consent Manager must publish on its website or app, or both, the period for responding to the grievances under its redressal system.



9

Additional Elements of data security

The Rules also emphasizes on additional specific security aspects in parallel to provisions of breach

Reasonable Security Safeguards

Data Fiduciaries are required to implement security measures to safeguard personal data. These measures include encryption, access controls, monitoring for unauthorized access, data backups, and other protections to maintain the confidentiality, integrity, and availability of data. They must also detect and address breaches while maintaining detailed logs. Additionally, contracts with Data Processors must mandate appropriate security measures.

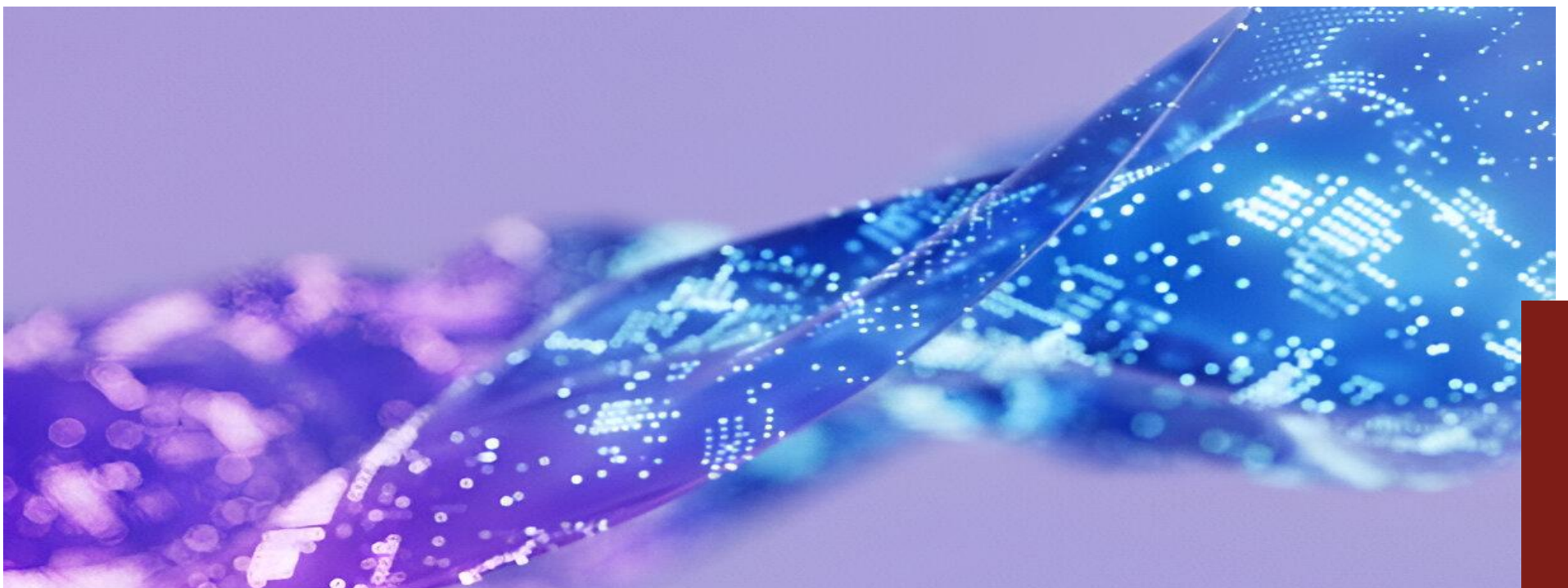
Cross-Border Data Transfer or Processing

The transfer of personal data outside India by a Data Fiduciary, whether processed within or outside India for offering goods or services to Indian Data Principals, is subject to the following restriction - Such transfers must comply with requirements specified by the Central Government through general or special orders, particularly when making data available to foreign states or entities under their control.

Calling for Information from Data Fiduciary

The Central Government, through authorized persons specified in the Seventh Schedule, can request information from Data Fiduciaries or intermediaries for purposes outlined in the Act. The rule allows the Government to:

- Specify the timeframe for providing the requested information.
- Restrict the disclosure of such information if it could adversely affect India's sovereignty, integrity, or state security.



10

The Data Protection Board

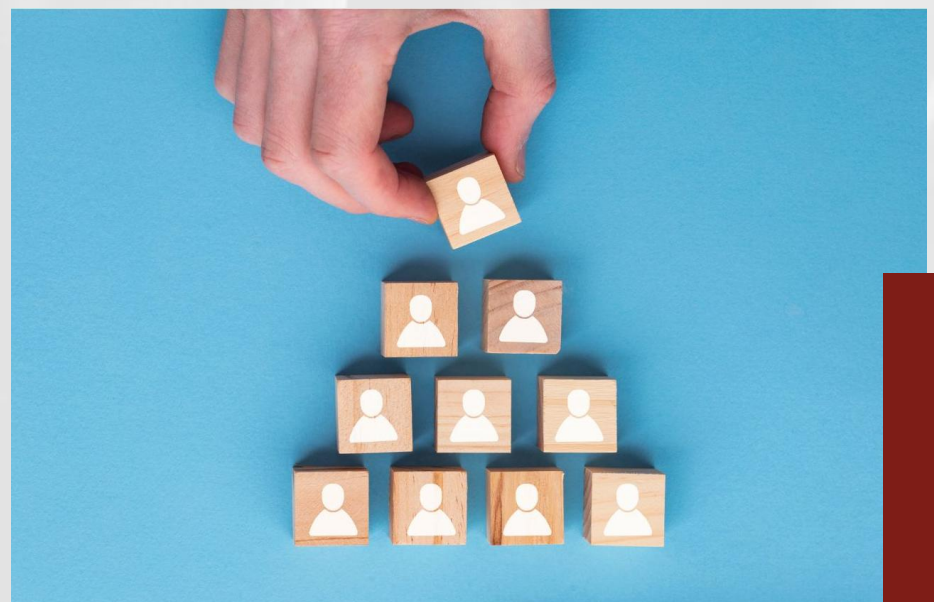
The Rules detail out the appointment of the Board members and its officers, the proceedings of the Board, the requirement to be techno-legal, and on appeal

Noteworthy points

- ❖ A Search-Cum-Selection Committee shall recommend eligible individuals who can become the Chairperson of the Board. A separate Committee shall also recommend suggestions for Members of the Board. The Central Government will, after considering the suitability, finally appoint the Board's Chair and Members.
- ❖ The Board constituted shall, with prior approval of the Central Government, appoint officers and employees for the efficient discharge of its functions.
- ❖ The Board is mandated to integrate techno-legal measures for digital efficiency in its operations.
- ❖ The Board's members, including the Chair, as well as the officers, have to be public servants, including from any government service, PSUs, or autonomous government institutions. (DPDP Act)

Appeal

- ❖ Appeals by an aggrieved person against the Board's orders or directions must be filed digitally as per the procedures on the Appellate Tribunal's website, and subject to a fee of like amount as applicable under TRAI Act 1997.
- ❖ The Rules mandate that the Appellate Tribunal shall operate independently of the Civil Procedure Code, 1908, adhering instead to principles of natural justice and regulating its own procedure. It should embrace, again, techno-legal measures for digital operations, ensuring the right to be heard without necessitating personal presence.



Primus' Take

The Draft DPDP Rules, 2025, reflect a decisive step forward in operationalizing the DPDP Act, 2023, by establishing clear and actionable guidelines for Data Fiduciaries, intermediaries, and the State. These rules are poised to enhance accountability, foster trust among citizens, and strengthen India's digital economy. They are grounded in the principles of fairness and proportionality, and set a strong foundation for safeguarding personal data in a rapidly growing digital ecosystem.

The emphasis on clear, plain-language notices demonstrates the intent to empower individuals by enabling informed decision-making. For businesses, this will require investments in legal and technological expertise to meet compliance standards. While larger enterprises are well-equipped to adopt these changes, the rules present an opportunity for smaller businesses to elevate their data protection frameworks and build trust with users.

The State-led data processing for subsidies and benefits, reinforces the government's commitment to accountability and transparency in its dual role as a regulator and processor. By linking such processing to the standards outlined, including data minimization, accuracy, and security safeguards, the rules ensure that State entities align with the same principles expected of private entities. This will strengthen citizen confidence in government-led data initiatives while supporting seamless service delivery.

The rules' approach to breach notifications strikes a balance between urgency and practicality, ensuring that both regulators and affected individuals are informed in a timely manner. However, the existing frameworks under the IT Act and CERT-In reporting guidelines highlight the importance of harmonized reporting mechanisms to reduce duplicative efforts. A unified portal for breach notifications, which enables streamlined compliance, could further strengthen the implementation of this rule.

Significant Data Fiduciaries (SDFs) are entrusted with higher accountability, including annual Data Protection Impact Assessments (DPIAs), algorithmic due diligence, and restrictions on cross-border data transfers for specified categories of data. These obligations will instill a culture of proactive data governance, ensuring that entities handling large volumes of personal data maintain rigorous safeguards. At the same time, the implementation has to be such that it does not compromise innovation.

Rules also hold significant implications for the development and deployment of Artificial Intelligence (AI) in India. By mandating robust data protection standards, such as algorithmic due diligence, the rules ensure that AI systems rely on ethical and secure data practices. This not only safeguards individuals' rights but also builds trust in AI-driven innovations. Furthermore, the focus on 'need-based' data localization and sovereignty strengthens India's position as a global AI hub, encouraging domestic development while enabling the use of personal data for socially beneficial AI applications within a well-regulated framework.

Overall, the Draft DPDP Rules, 2025, showcase a forward-looking vision that balances the needs of individuals, businesses, and regulators. For businesses, these rules provide clarity and certainty at most level, enabling them to align their operations with India's regulatory environment. For citizens, the rules enhance trust by prioritizing transparency, accountability, and safeguards for personal data.

PRIMUS

PASSION

for providing solutions to help clients achieve their goals

RESPECT

for all and alternate viewpoints

INTEGRITY

of thoughts and actions

MASTERY

of our chosen subject to drive innovative and insightful solutions

US

representing the Primus collective, where each individual matters

STEWARDSHIP

for building a better tomorrow



PRIMUS PARTNERS®

Solutions for Tomorrow

Primus Partners has been set up to partner with clients in 'navigating' India, by experts with decades of experience in doing so for large global firms. Set up on the principle of 'Idea Realization', it brings to bear 'experience in action'. 'Idea Realization'— a unique approach to examine futuristic ideas required for the growth of an organization or a sector or geography, from the perspective of assured on-ground implementability.

Our core strength comes from our founding partners, who are goal-oriented, with extensive hands-on experience and subject-matter expertise, which is well recognized in the industry. Established by seasoned industry leaders with extensive experience in global organizations, Primus Partners boasts a team of over 250 consultants and additional advisors, showcasing some of the finest talent in the nation.

The firm has a presence across multiple cities in India, as well as Dubai, UAE. In addition, the firm has successfully executed projects across Africa, Asia Pacific and the Americas.

This document has been drafted by Primus' Public Policy Realization team.

India Offices

 **Bengaluru**

91 Springboard
Business Hub 175, 176
Bannerghatta Rd,
Dollars Colony,
Bengaluru – 560076

 **Chandigarh**

2nd Floor, Netsmartz,
Plot No. 10, Rajiv
Gandhi Chandigarh
Technology Park,
Chandigarh – 160019

 **Chennai**

147, Pathari Rd, Door #3,
WorkEz Hansa Building,
RK Swamy Centre,
Thousand Lights,
Chennai, TN - 600006

 **Delhi**

1 to 7, UG Floor,
Tolstoy House,
Tolstoy Road,
Connaught Place
New Delhi - 110001


 **Kolkata**


Siddhartha Apartments
4th Floor, 188/2,
Block J,
New Alipore,
Kolkata - 700053


 **Mumbai**


601, 6th floor,
Raheja Centre,
Nariman Point,
Mumbai,
MH - 400021


International Offices


 **Dubai**
United Arab Emirates


 **Dammam**
Kingdom of Saudi Arabia

 www.primuspartners.in

 info@primuspartners.in

 Primus Partners India

 @partners_primus

 @primuspartners7128