



Centre for
Knowledge
Sovereignty[®]

MOM of CKS Internal Discussion on Draft DPDP Rules 2025

-Chatam House

Date: 11 January 2025



Time: 11:00 hrs to 13:00 hrs

Platform: Zoom

Attendees:

1. Lt Gen Dr D B Shekatkar
2. Lt General Vinod Bhatia
3. Lt. General Vinod Khandare
4. Shri Vinit Goenka
5. Major General Rajan Kochhar
6. AVM Pranay Sinha
7. Dr. K. J. Ramesh
8. Dr G.Shreekumar Menon
9. Wing Commander Deepak Prasad
10. Col V.D.Singh
11. Col Virendra Kumar
12. Shri Sunil Agarwal
13. Dr Deepa Prakash
14. Shri Agendra Kumar
15. Shri Ashok Narayanswamy
16. Dr Vijay Rai
17. Shri Saurabh Rai
18. Mrs Sumitra Goenka
19. Shri Gaurav Tripathi
20. Shri Gaurav Mishra
21. Dr Sunil S Bhat
22. Dr Munesh Chandra Trivedi
23. Shri Piyush Prasoon
24. Ms. Lekshmi Parameswaran
25. Ms. Kriti Sinha
26. Dr Kriti Singh

Minutes of the Meeting

I. Data Privacy and Sovereignty

1. Data leaving the country poses a greater risk compared to data entering.

2. Data sovereignty, residency, and localization need deeper debate and incorporation into the rules.
3. Definition of what constitutes Personal data privacy must be explicitly incorporated in the DPDP rules.
4. The current draft is insufficiently focused on data sovereignty and data propriety.
5. Indian companies should map sensitive zones to ensure the data remains within the country.
6. Locational and Geospatial data must be included in the framework.

II. Consent and Data Protection

1. The use and violation of data without a person's consent highlight a serious issue.
2. The Dos and don'ts of data sharing must be widely publicized.
3. Clear timelines for obtaining and renewing consent for data collection are necessary.
4. A mechanism for withdrawing consent and data must be defined.
5. Stringent laws and penalties are needed to address the misuse of personal data, particularly by e-commerce platforms.
6. There must be strict guidelines to protect sensitive data that cannot be shared.
7. Schools sharing data with coaching institutes is an issue—rules should cover digital and physical data.

III. Regulatory and Institutional Frameworks

1. NTRO's role and responsibilities should be defined in the bill.
2. The Data Protection Board's authority and effectiveness must be reviewed.
3. Consideration should be given to establishing a Data Tribunal with judicial powers to address violations and enforce penalties.

4. A central agency should monitor data collection, sharing, and storage with mandatory prior permission before accessing data.
5. Mechanisms for regular review and updates of the DPDP Act should be established.

IV. Technological Concerns and Measures

1. A robust technological architecture is needed to safeguard data.
2. Encryption of all shared data across platforms must be mandated.
3. Regular security audits should be implemented.
4. The incorporation of AI and blockchain technology in data management is essential.
5. Geo-referencing of data and geo-fencing of sensitive data must be prioritized.
6. Indian platforms should be optimized and encouraged for data handling under the Atma Nirbhar Bharat initiative.

V. Industry and Compliance

1. Data fiduciaries need clearer mandates and guidelines on record maintenance.
2. Compliance for small businesses and startups is challenging; readymade solutions must be available.
3. The rules must create a level playing field for big tech and startups.
4. The issue of economic theft must be addressed, and there must be no buying or selling of data without proper checks.
5. Trusted jurisdictions for data transfers need to be defined with clarity.

2. Children's data on e-commerce platforms and gaming sites requires more attention and deliberation.
3. Medical data collected during camps is not adequately protected.
4. Misuse of data should not harm national progress; stringent laws and severe punishments are required.
5. False Aadhaar cards and data poisoning must be addressed as serious offenses through legislation.
6. Glaring corrupt practices, such as the illegal sharing of medical information, must be eliminated.

VII. Awareness and Education

1. The government must initiate public awareness programs on data protection.
2. Data literacy should be a prerequisite for government job applicants.
3. Law enforcement agencies should be educated on data protection laws and practices.

VIII. Opportunities and Challenges

1. India must align with a global framework for data sharing and agreements.
2. Data should be seen both as an opportunity and a challenge, optimized for public well-being.
3. The DPDP Act is an evolving framework and will likely undergo multiple amendments.

IX. Specific Issues

1. Unregulated content on platforms like YouTube poses risks that need to be addressed.
2. Chinese cameras in sensitive locations raise national security concerns; a regulatory framework is needed.

3. Data collected by foreign vehicle service centers is uploaded without clear legal oversight.
4. Mechanisms to verify the authenticity of uploaded data are missing.
5. Timelines for implementing the act and rules need to be specified.

X. Proposals for Improvement

1. Introduce penalties for e-commerce sites that misuse personal data.
2. Establish stringent laws against data misuse to prevent harm to individuals and national interests.
3. Define clear provisions for the withdrawal and renewal of data consent.
4. Promote indigenous platforms to reduce dependency on foreign systems.
5. Emphasize technological sovereignty through regulatory measures.
6. Educate and train individuals on data protection, focusing on law enforcement and public servants.
7. SMEs and Startups interest to be protected.

XI. Actionable Points

1. Each participant is encouraged to introduce five individuals to CKS to enhance the depth and diversity of discussions.
2. Feedbacks be taken from cross section of people.
3. Participants must share their insights and suggestions via email or WhatsApp by 20 January 2025. These contributions will be consolidated into a comprehensive document for submission to the ministry.
4. Core group to be formed and a 1–2-page summary of our recommendations be provided to GOI before 10 February 2025.



Centre for[®]
Knowledge
Sovereignty



<https://www.linkedin.com/company/cksindia/>



<https://x.com/CKSIndia>



https://www.youtube.com/@CKS_INDIA



www.cksindia.in