cyril amarchand mangaldas
ahead of the curve

fig bulletin

a quarterly newsletter by cam financial institutions group

January - March 2025

Index

It gives us immense pleasure to share with you the ninth issue of the Financial Institutions Group (**FIG**) *Bulletin*, a quarterly newsletter produced by our FIG practice.

This edition captures key regulatory shifts across India's financial landscape. The Reserve Bank of India (**RBI**) advanced reforms on financial disclosures, cross-border payment security, and Indian Rupee (**INR**)internationalization. Securities and Exchange Board of India (**SEBI**) introduced safeguards for retail algorithmic trading and enhanced system audit protocols. Insurance Regulatory and Development Authority of India (**IRDAI**) enabled equity derivative hedging and launched UPI-based premium mandates to streamline insurance payments. The International Financial Services Centres Authority (**IFSCA**) strengthened governance in bullion markets, clarified remote trading norms, and proposed frameworks for tokenizing real-world assets. Collectively, these updates reflect a strong regulatory push toward transparency, innovation, and resilience in the financial ecosystem.

We hope you enjoy reading this newsletter. Please feel free to send your comments, feedback and suggestions to cam.publications@cyrilshroff.com

Regards,

Cyril Shroff

Managing Partner
Cyril Amarchand Mangaldas

India's leading law firm

Draft Digital Personal Data Protection Rules, 2025 – Key Implications for Financial Services Sector[1]

Background

1. India's first dedicated data privacy law, the Digital Personal Data Protection Act, 2023 (**DPDP Act**)[2], was passed by both houses of Parliament, and received Presidential assent on August 11, 2023.

2. The DPDP Act aims to regulate the processing of digital personal data, outlining requirements for collection, processing and sharing of personal data. It also specifies the rights of data principals (right to correction, erasure, etc.), processing of children's data, obligations of data fiduciaries and other related matters. The DPDP Act is yet to be notified and requires promulgation of Rules, basis which the Central Government will notify the DPDP Act.

3. The Ministry of Electronics and Information Technology (**MeitY**) published the draft Digital Personal Data Protection Rules, 2025, on January 3, 2025 (**Draft Rules**), inviting feedback/ comments from stakeholders. The last date of submission of feedback on the Draft Rules to MeitY is February 18, 2025[3].

4. The DPDP Act contemplates 25 instances for the Central Government to frame and notify Rules, including manner of consent notice, form and manner of intimation of data breach, manner of obtaining verifiable consent, obligations of significant data fiduciaries, obligations of consent manager and establishment of the Data Protection Board (**Board**). The Draft Rules cover each of these aspects.

Our earlier FIG Papers on the DPDP Act and its impact on the banking, financial services and insurance (**BFSI**) sector can be accessed: (i) Financial Services Implications – here; (ii) Implications on Payment Service Providers – here; (iii) Implications on Banks – here; (iv) Implications on Asset Management Companies – here; (v) Implications on Foreign Banks – here; and (vi) Implications on Non-Banking Financial Companies – here.

Key Features & Analysis

1. Consent Notice:

   - *Rule 3, Draft Rules*: Requires the consent notice to be given to a data principal to be "presented and be understandable independently" and at a minimum, to include, (a) itemised description of personal data being collected, and (b) "goods or services to be provided or uses to be enabled by" processing of the personal data.

   - *Corresponding DPDP Act Section (S. 5)*: Requires a consent notice prior to collection of personal data, informing: (a) the purpose for collection; (b) manner of exercise of rights under the act; and (c) manner of making complaint to the Board.

   - *Analysis*: The requirement of consent notice to be "presented independently" means that consent notices cannot be bundled with any other engagement with a data principal, such as customer on-boarding form, agreement, privacy policy, etc.

2. Consent Manager:

   - *Rule 4, Draft Rules*: Prescribes eligibility criteria and obligations of Consent Managers, which include a company incorporated in India, net-worth requirement of INR 2 crore, adequate earning prospects, sufficient capacity, good character of management, and good financial condition.

   - *Corresponding DPDP Act Section (S. 6(7))*: The DPDP Act introduced the 'Consent Manager' regime, as a single point of contact to enable data principals to give, manage, review, and withdraw their consent.

   - *Analysis*:

     - The Draft Rules give flexibility to BFSI entities (banks and non-banks) and tech companies/ platforms to have a group-wide consent manager, provided there is no conflict of interest

1 FIG Paper (No. 40 – Data Law Series 6) Draft Digital Personal Data Protection Rules, 2025 - Key Implications for Financial Services Sector | India Corporate Law
2 Available here.
3 The feedback is to be submitted online through MyGov portal, accessible at the link (here).

between a data fiduciary and Consent Manager's directors, key managerial personnel and senior management[4].

- This creates an opportunity for entities, especially those in the BFSI space, and in particular the Reserve Bank of India (**RBI**) licensed non-banking financial company – account aggregator, to enter into a new line of business as 'white-label' consent managers.

3. Overseas Processing/ Data Transfer:

- *Rule 14, Draft Rules*: Requires that transfer of personal data outside India must comply with the requirements to be laid down by the Central Government, if data is being transferred to a 'foreign State' or to any person or entity under the 'control' or any agency of such State.
- *Corresponding DPDP Act Section (S. 16(1))*: The Central Government has the power to restrict the transfer of personal data to a country/ territory outside India, by way of a notification.
- *Analysis*:
  - The above is a departure from the DPDP Act, which envisaged a negative list of countries, to which personal data cannot be transferred.
  - Assessment in relation to treatment as 'foreign State' would require local law inputs.

4. Data Breach:

- *Rule 7, Draft Rules:*
  - In addition to the Indian Computer Emergency Response Team (**CERT-In**), data fiduciaries must report the breach of personal data, without delay, from becoming aware of the breach, to:
    - data principals – description of breach, relevant consequences for data principal, risk-mitigation measures implemented, safety measures that the data principal may take and information of the data protection officer; and
    - the Board – nature, extent, timing and location of occurrence and the likely impact;
  - Whilst the above reportings are to be made simultaneously, the information to be included in both these reports are not harmonised.
  - Within 72 hours from becoming aware of the breach, additional details, including updated and detailed information, broad facts related to the events, risk-mitigation measures implemented, any findings regarding the person who caused the breach, remedial measures taken to prevent recurrence, and a report regarding intimation to the affected data principals are to be submitted to the Board.
- *Corresponding DPDP Act Section (S. 8(6))*: Requires that a data fiduciary must report a data breach to the Board and the data principal, in such manner, as may be prescribed.
- *Analysis*: For BFSI entities (banks, non-banks, payment service providers, asset management companies, other intermediaries and outsourced service providers), this means reporting has to be made to, (a) respective sectoral regulator (RBI, Securities and Exchange Board of India and Insurance Regulatory and Development Authority of India), (b) CERT-In, (c) data principal, and (d) the Board – regarding the breach, with different timelines and content for each such reporting.

5. Specified Purpose:

- *Rule 8, read with Third Schedule, Draft Rules:* A three-year period has been prescribed, after which the specified purpose would be deemed to be no longer being served (after which personal data must be erased) for the following entities:
  - e-commerce entity with not less than two crore users in India;
  - online gaming intermediary with not less than 50 lakh users in India; and
  - social media intermediary with not less than two crore users in India.

[4] Paragraphs 9 and 10, Part B, First Schedule, Draft Rules.

- *Corresponding DPDP Act Section (S. 8(7) and 8(8))*: Prescribes that a data fiduciary must erase personal data of a data principal "as soon as it is reasonable to assume that the specified purpose is no longer being served", and requires the Central Government to prescribe the time period and classes of data fiduciaries (along with purposes), for which specified purpose is no longer deemed to be served.
- *Analysis*: The three-year time has been prescribed only for the above stated entities. It does not extend to regulated entities (banks, non-banks, payment service providers, asset management companies and other intermediaries) and would require further clarity from MeitY for data retention periods applicable to them.

6. Reasonable Security Safeguards:

- *Rule 6, Draft Rules*: Prescribes minimum security safeguards to prevent personal data breaches, including data security measures (securing data through encryption and virtual tokenisation), access control measures and visibility on access to personal data, reasonable measures for continued processing in the event of compromise, for detection of unauthorised access and appropriate technical and organisational measures to ensure observance to security safeguards.
- *Corresponding DPDP Act Section (S. 8(5))*: Requires data fiduciaries to protect personal data in its possession, by taking reasonable security safeguards.
- *Analysis*:
  - The prescribed security measures are in line with the existing financial services sectoral regulations and global security standards adopted by technology companies/ platforms and BFSI entities.
  - Non-regulated entities, especially IT/ ITeS platforms, would have to create and implement reasonable security safeguards as above, which is likely to be time and cost intensive.

7. Significant Data Fiduciaries (**SDF**):

- *Rule 12, Draft Rules*:
  - Requires that upon being classified as SDF, a Data Protection Impact Assessment (**DPIA**) be undertaken and a report containing 'significant observations' must be submitted to the Board. DPIA is required to be conducted on an annual basis.
  - SDFs to ensure that such personal data, as may be specified by the Central Government (on the basis of recommendations of a committee), is processed subject to restriction that the personal data and traffic data is not transferred outside India[5].
- *Corresponding DPDP Act Section (S. 10(1) and 10(2))*: Lays down the indicative criteria basis which the Central Government may notify any data fiduciary or a class of data fiduciaries as SDFs, including:
  - the volume and sensitivity of personal data processed;
  - risk to the rights of Data Principal;
  - potential impact on the sovereignty and integrity of India;
  - risk to electoral democracy;
  - security of the State; and
  - public order.

It also grants power to the Central Government to prescribe additional obligations for SDFs.

- *Analysis*:
  - 'Significant Data Fiduciaries' have not yet been notified by the Central Government.
  - The Draft Rules give the Central Government power to specify the nature of personal data that would have to be localised in India – an absolute bar on transfer outside India. This seems to be a departure from the DPDP Act to not impose a data sovereignty rule.

[5] Rule 12(4), Draft Rules.

To read the complete newsletter, please visit our website

https://www.cyrilshroff.com/newsletters