# Draft DPDP Rules: Heightened data concerns for financial sector entities.

- Subhojit Shome, Archisman Bhattacharjee, Aditya Iyer (*finserv@vinodkothari.com*)

**Table of Contents**

## Background

On January 03, 2025, the Ministry of Electronics and Information Technology ('MeitY'), published the Draft Digital Personal Data Protection Rules, 2025 ('DPDP Rules') nearly 16 months and a half after the Digital Personal Data Protection Act, 2023 ('DPDPA') was enacted. Salient features of the DPDP Rules include notice by Data Fiduciary ('DF') to Data Principal ('DP'), obligations of the consent managers, data security and reasonable safeguards, intimation of personal data breach, and provisions relating to data of children and persons with disability who have a lawful guardian.

Currently, there are no immediate actionables, as the DPDP Rules are still draft rules and will be taken up for consideration only after February 18, 2025. Further, Rule 3 as well as Rule 6, which may particularly relate to financial sector entities, shall come into force only from a date to be specified, which indicates that the intent of MeitY is to give sufficient preparation time.

However, as compliance with the DPDP Rules would require lenders to draft/ re-draft/ amend documents (such as loan documents, and service agreements), engineer features into their website (e.g. pertaining to withdrawal of consent), and create institutional mechanisms, it would be very prudent for the concerned entities to take note of the same, and brace themselves for the implementation.

In this note, we comment on certain key-aspects of the DPDP Rules insofar as they are relevant for financial sector entities, along with the statutory context, and our views on implementation / other applicable compliances. For an introduction to the DPDPA, and considerations for financial sector entities, *see* our explainer on the impact on digital lenders, here, and our break-down of the consent manager norms, here.

## Analysis of key rules and concerns for lenders

### 1. Notice of use of personal data - Rule 3

**DPDPA Context**: Section 6 of the DPDPA, *inter alia*, requires that the consent given by the 'DP' (i.e. the individual to whom the personal data relates) to the DF (i.e. the person determining means and purpose of processing data) shall be free, unambiguous and specific. Further, as per Section 5 of the DPDPA, the request for consent to the DP shall be made with an accompanying notice ('Notice') that shall outline aspects such as the purpose, the manner in which DP can make a complaint to the Board.

**DPDP Rules**: The DPDP Rules require that the Notice shall be made, and be understandable, independently of other information that has been, or is made available, by DF. In addition, the Notice should be in a clear and plain language, with an "itemised description" of personal data, and an itemised description of the goods/services for which the data may be processed. It shall also contain the means by

which the DP can withdraw their consent, access the website of the DF, and exercise rights under the DPDPA including but not limited to the right of withdrawal of consent

**Implications for lenders**: Where consent needs to form the basis of processing information, lenders would be required to give Notice for the same as per the DPDP Rules. Common scenarios this may be implicated in, and factors for consideration, are as below:

(a) **Cross-selling and cross-marketing**: A lender/LSP using data for cross-selling products to the borrower would need to give notice for the same. This would also be pertinent for entities engaged in cross-marketing. In the case of cross-marketing, the data / insights generated from customer data, are used to pitch the customer other products (which may include the products of third-parties, with whom the lender has a tie-up). For e.g., at the time of extending a credit facility, it is identified that the customer has a house in an upmarket, and prime area. Accordingly, a Loan Against Property (i.e. a LAP) is pitched to the customer. Such concerns would also be implicated where the borrower data is being sold to third-parties.

(b) **To be independent of other information**: As per the DPDP Rules, the notice cannot simply be integrated into the larger text of the Loan Agreement / MTC, as a general clause such as "borrower hereby agrees". Thus, the notice should not be buried under a mountain of other consents, and be opaque. Instead, a clear and unequivocal accompanying document, along with sanction letter and loan agreement, may be provided to the borrower.

(c) **Microfinance lending**: In the case of microfinance loans particularly, it is also important that this Notice be tailored to the demographic profile of borrowers (such as the vernacular language). Additionally, if borrowers belong to groups with low literacy rates, then it may also be accompanied with explanations by the DSA/ DMA to fulfill the requirement in letter and spirit.

(d) **Itemised description:** The Notice so provided to the DP should contain an itemised description of the personal data, and the goods and services, or uses to be enabled, by such processing. An itemised description would entail a list of the personal data collected by the DF, from the DP, and a list of items that data will be processed for. For instance, where the lender has obtained the contact information of the borrower (such as their email ID and phone number), and should they use that data to cross-market services, then such purpose should be disclosed in the list beforehand. Similarly, where the borrower's data is being used for the purposes of generating demographic based analytics, that too would need to be disclosed.

(e) **Guidelines on Digital Lending**: It is also important to read the requirement of providing an itemised description with the Guidelines on Digital Lending ('DL Guidelines'). Under the DL Guidelines, there is a requirement that explicit consent of the borrower shall be taken, before sharing the information with any third-party, except for cases where sharing is pursuant to a regulatory requirement (Para 10.4 of DL Guidelines). Additionally, there is a requirement that the details of third-parties allowed to collect information through the Digital Lending App shall be disclosed in the privacy policy (Para 12.2 of DL Guidelines). One practice has been to read these together, and capture in the loan documents a clause obtaining borrower's consent for sharing information to certain parties, with a hyperlink, where such parties are listed. Under the DPDP Rules, this practice will no longer be permissible. In case data is being shared with a new party,

for a purpose other than the legitimate purpose, then consent from the borrower would need to be obtained for the same with the corresponding itemised description.

Additionally, since the Notice as per the DPDP Rules should be "understandable", lenders should read this with the Fair Practices Code (under the SBR Directions), which requires for all communications to the borrower being in vernacular language, or language as understood by the borrower.

**A note on Notice**: It should be noted that the requirement of providing the Notice to the DP arises only in cases where consent is the basis of processing of information and the same may not be required to be provided where processing of information is based on processing for purposes as listed out in Section 7 and Section 17 of the DPDPA.

Section 7 envisages a range of exceptions, exempting lenders from obtaining specific consent and giving the notice. Where for instance, the personal data of the borrower is being used to carry out KYC/credit-appraisal, then such processing of personal data would fall under Section 7(a).

However, as mentioned above, where the data is being processed for other purposes (such as cross-selling, cross-marketing, analytics, etc.), then Notice as per the DPDP Rules would need to be given.

Crucially, it should be noted that the requirements of implementation of reasonable security standards as provided under Rule 6 read along with Rule 8(5), is not waived due to the non-requirement of the providing of such notice, and the DF shall be responsible for all processing that is carried out by the DF or a DP on its behalf.

**Penalties**: As per Section 33(1) of the DPDPA, read with the Schedule of the DPDPA, the DF's penalty for failing to give the DP notice of use of personal data, may extend to ₹50 crore.

## 2. Reasonable security safeguards - Rule 6

**DPDPA Context:** Section 8 of the DPDPA clarifies that the DF would be responsible for complying with the provisions of the DPDPA, irrespective of any agreement to the contrary/failure by the DP. This is to say that, the rights granted under the DPDPA to the DP cannot be "contracted-away". Additionally, Section 8 requires that the DF shall process the personal data under its control by taking "reasonable security safeguards" to prevent personal data breach

**DPDP Rules**: As regards the "reasonable security safeguards", the DPDP Rules require that the reasonable security safeguards, shall at a minimum include securing the personal data through encryption, limiting the access to computer resources used by such DF, enabling prompt detection of unauthorized access, and also ensuring continuity in processing in case of cyber breaches. The DPDP Rules also require that appropriate covenants be included in the contract between the DF and the Data Processor (i.e. person who processes personal data on behalf of the DF) for such purpose. Under Rule

(g), a mandate has been placed upon the DF to implement technical and organizational measures to ensure compliance with the same.

**Implication for lenders**:

(a) In our view, for NBFC-ML entities, to the extent of IT services being outsourced, this may be read with the extant guidelines under the IT Outsourcing Directions, as well as the Business Continuity Plan (BCP) and Disaster Recovery Drills (DR Drills) norms under the IT Governance Directions. For NBFC-BL the norms the BCP and DR drill norms as captured under the 2017 IT Directions, would be applicable. The aforementioned BCP and DR drill requirements applicable upon lenders, is co-extensive with obligations under DPDP Rules with respect to ensuring continuity in processing.

(b) Further it should also be noted that the application of the DPDPA as well as the DPDP Rules will not be limited to outsourcing of the IT function, but also to all financial outsourcing as well as vendors with whom personal data might have been shared irrespective of the activity amounting to financial service outsourcing and IT Outsourcing. Accordingly, all precautions as has been provided under the DPDP Rules, read along with the DPDPA, will need to be complied by the DF.

(c) For IT services, placing reliance on a Data Processor, by applicable financial sector DF (such as Banks and NBFCs-ML/UL), would in most circumstances be considered "IT Outsourcing" as per the IT Outsourcing Directions, and thus, under Para 16 of the IT Outsourcing Directions, the DF is mandated to include certain clauses in its Service Agreement with such Data Processor. These clauses include obligations pertaining to reasonable security safeguards, and *inter alia* include a mandate on the Data Processor to ensure regular monitoring of the activities, compliance with applicable IT laws, having a contingency plan in place, and maintaining controls to ensure confidentiality of the DP.

(d) Furthermore the requirement of reasonable security safeguards by the DP shall not only be limited to incorporating respective clauses in the outsourcing agreement but also include the process of carrying out a Vendor Privacy Risk Assessment ('VPRA') prior onboarding of any of such vendors. The VPRA shall include assessment of the privacy safeguards that have been implemented by the vendor to be onboarded. While the requirement to conduct a VPRA is not explicitly mandated by the DPDPA or the DPDP Rules, it is important to highlight that under Section 8 of the DPDPA, the DF bears responsibility for all processing activities performed by the DP. Consequently, any failure on the part of the DP to implement reasonable security safeguards could result in significant penalties being imposed on the DF, as outlined below.

To mitigate such risks, it is advisable for the DF to conduct a VPRA prior to onboarding any DP. This assessment would ensure that the DP's security measures are commensurate with the sensitivity of the personal data involved and aligned with the potential risks associated with its processing.

**Penalties**: As per Section 33(1) of the DPDPA, read with the Schedule of the DPDPA, the DF's penalty for failing to take reasonable security safeguards may extend to ₹250 crore.

## 3. Intimation of personal data breach - Rule 7

**DPDPA Context:** As per Section 8(6) of the DPDPA in event of any personal data breach the DF is required to intimate the DP as well as the Data Protection Board ('DPB') regarding the breach. However the timelines within which such intimation is required to be provided was not provided under the DPDPA and the same was supposed to be prescribed under the DPDP Rules.

**DPDP Rules**: Under the DPDP Rules it has been intimated that the DF is required to intimate the DP without any delay about the data breach incident and simultaneously the same should also be notified to the DPB. Further under rule 7(2) of the the DF is also required within a period of 72 hours (except in cases where extension of the timeline has been provided by the DPB) towards the updates of the data breach incident which shall include the measures that has been implemented by the DF to contain/mitigate the risk, information regarding persons who have caused the breach, remedial measures taken to prevent recurrence of the breach and a report regarding the intimations given to the affected DP.

**Implication for lenders:** The Lender is required to prioritize the rights and interests of the DP (individuals whose data has been breached). Key responsibilities include:

(a) Timely Intimation: The lender must notify each affected DP without undue delay. However, in our view "without delay" does not necessarily mean an immediate notification to the DP as soon as the breach is detected. Instead, the NBFC's primary focus should be on mitigating the risk associated with the breach. The NBFC should promptly implement measures to minimize the impact of the breach and ensure that only the minimum amount of personal data is compromised. Once these mitigation measures are underway, the notification to the affected DPs should be sent without further delay, ensuring they are informed while the breach is being addressed effectively.

However for all intents and purposes the notification should be sent to the borrower within a period of 24 hours from the time the breach had been observed by the DF. Regarding the mitigation measures that are required to be implemented by lenders, it should be noted that in accordance with Para 27(d) of the IT Governance Directions, lenders are required to have a cyber incident response plan and recovery management policy in place and in case of any cyber breach the lenders should ensure to adhere to the requirements of Para 27(d) to avoid regulatory scrutiny, and penalties under the DPDPA.

(b) Details to be Communicated:
- Nature, extent, timing, and location of the breach.
- Potential impacts on the individual resulting from the breach.
- Measures implemented or being implemented by the DF to minimize risks.
- Steps the DP can take to protect their interests, such as securing accounts or changing passwords.

- Business contact details of a representative who can address queries or provide assistance. (Refer DPDP Rule 9)

(c) Notifications must be sent through the individual's registered user account or other communication methods provided to the DF ensuring accessibility. The user account as used above means the online account registered by the DP with the DF, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such DPl is able to access the services of such DF.

(d) The lender's engagement with the Data Protection Board is two-fold, ensuring immediate reporting and comprehensive follow-up. As regards immediate reporting, see key-points below:
- The Board must be informed without delay once the breach is discovered.
- The initial report should include a description of the breach, covering its nature, extent, timing, location, and likely impact.
- A more detailed submission must be provided within 72 hours of discovering the breach. This can be extended with written approval from the Board. The submission should include:
    a) Updated information: A refined description based on investigations.
    b) Broad facts: Key details about events, circumstances, and reasons leading to the breach.
    c) Risk mitigation measures: Steps taken or proposed to reduce harm.
    d) identifying the cause: Findings about the person or factors responsible for the breach.
    e) Remedial measures: Actions implemented to prevent recurrence.
    f) Affected individuals report: Details of the notifications sent to DPs.

**Other factors/implications:** In addition to notifying the DP, the NBFC is also required to inform CERT-IN within six hours of becoming aware of the data breach, in compliance with notification No. 20(3)/2022-CERT-IN. Further in accordance with para 27(d) of the IT Governance Master Directions notification is also required to be sent to the RBI.

It is important to note that DPDP Rule 7 extends beyond breaches involving the lender's own systems. The NBFC must also notify the DP and the DPB in cases where the breach occurs within the systems of its Data Processor. This requirement arises because, under Section 8(5) of the DPDPA, the DF remains accountable for all processing activities carried out by its Data Processor. Further an obligation to notify the RBI also arises out of Para 17(i) of the IT Outsourcing Directions, directing applicable entities to immediately notify the RBI in case of breach of security/leakage of confidential information, with respect to data stored/processed by service providers (which would likely include the Data Processor)

**Penalties**: A failure to notify the DP regarding the personal data breach, shall attract a penalty of ₹200 crore.

## 4. Time period for specified purpose to be deemed as no longer being served - Rule 8

**DPDPA context:** Section 8(7) of the DPDPA stipulates that the DF is required to delete the the personal data of the DP upon the DP withdrawing their consent or the specified purpose for which the consent was provided by the DP including consent under Section 7(a) of the DPDPA is no longer served. Further the DPDPA stipulates that the specified purpose would be deemed to no longer be served under the following circumstances:

a. If the DP has not approached approach the DF for the performance of the specified purpose; and
b. If the DP does not exercise any of her rights in relation to such processing,

for such time periods as may be prescribed, and different time periods may be prescribed for different classes of DF and for different purposes.

**DPDP Rules**: A DF who is of a class as specified in the third schedule of the DPDP Rules, and processing data for such corresponding purposes, shall erase the personal data, unless its retention is required for compliance with applicable law, and unless the DP approaches the DF for performance of the specified purpose for which data is collected, or the DP exercises their rights in relation to processing of such data.

At-least forty-eight (48) hours before the completion of time period for erasure, the DF shall inform the DP that the data shall be erased unless the DP logs into their user-account, or approaches the DF for performance of the specified purpose, or else exercises their rights in relation to processing of such data.

**Implications for lenders:** The third-schedule is applicable upon e-commerce entities having not less than two crore registered users in India, online gaming intermediaries having not less than fifty-lakh registered users in India, and social-media intermediaries with not less than two crore registered users in India. Financial sector DFs (where applicable) would be primarily implicated through compliances prescribed for the first class, namely, e-commerce entities with not less than two crore registered users in India. This would apply for instance to NBFC-P2Ps, and also to other entities operating as intermediaries for purposes of facilitating lending through the marketplace model.

**Penalties**: Penalties for non-compliance with the same may extend to ₹50 crore .

## 5. Contact information about person to answer questions on processing - Rule 9

**DPDPA Context**: For ease of reference, the context has been presented in a tabulated form below.

| Section Number of DPDPA | Context |
|---|---|
| 8(10) | A DF shall establish an effective mechanism to redress the grievances of DPs. |

| | |
|---|---|
| 10(2)(iv) | A significant DF is required to appoint a Data Protection Officer who shall be the point of contact for the grievance redressal mechanism under the DPDPA |
| 13(1) | A DP shall have the right to have readily available means of grievance redressal provided by a DF in respect of any act or omission of such DF regarding the performance of its obligations in relation to the personal data of such DP or the exercise of her rights under the provisions of the DPDPA and the rules made thereunder. |
| 13(2) | The DF shall respond to any grievances referred to in 13(1) within such period as may be prescribed from the date of its receipt for all or any class of DF. |

**DPDP Rules:** The Rules require that the contact information of the person who shall be answering questions about processing be prominently published on the website and shall mention in every communication with the DP the business contact information of person appointed as Data Protection Officer/ 'DPO' (applicable for Significant Data Fiduciary/ 'SDF') or a person who is able to answer the questions on behalf of the DF.

**Implication for lenders:** Some key considerations for lenders are as follows:

(a) For lenders, it would be permissible to entrust the GRO with the function of answering questions about processing of data. The GRO here can be the existing GRO of the Company to whom the powers of addressing the grievances of the borrower may be provided. However it should be noted that usually for lenders the GRO who are appointed for the purpose of addressing lending relating queries/objections may not be technically competent to deal with privacy related issues and it would be of our suggestion that a separate GRO is appointed by the Company who is technically competent to address the issues or questions raised by the processing of personal data by the borrowers.

(b) As regards the DPO, we have shared elsewhere our view that, "In case regulated fintech entities are notified as SDFs, the question one may have is whether the GRO of such an entity can act as a Data Protection Officer. In our view, since the role of such an officer is to address grievances of the customers, specific to data protection, the role of a Data Protection Officer may be assigned to the GRO provided they are directly responsible to its Board of Directors." For more, *see* our write-up on the DPDPA here.

**Penalties**: Penalties for the same may range from ₹50 - ₹150 crore.

## 6. Rights of Data Principal - Rule 13

**DPDPA Context**: The following are the rights granted to the DP under the DPDPA:

(a) Right to withdraw consent - Section 6(4): Where the consent given by the DP is the basis of processing of personal data, then the DP shall have the right to withdraw consent at any time, with the ease of doing so being comparable to the ease with which consent was given.
(b) Right to grievance redressal Section 13: The DP shall have the right to readily available means of grievance redressal provided by the DF/Consent Manager, regarding performance of its obligations in relation to the personal data of the DP, or the rights of the DP under the DPDPA.
(c) Summary of Use and Sharing - Section 11: The DP shall have the right to request (through manner specified under the DPDPA), and receive, a summary of personal data being processed by the DF, as well as entities with whom such data is being shared, with a description of the data shared.
(d) Right to updation and correction - Section 12: The DP has the right to request updation and correction of personal data so shared with the DF.
(e) Right to nominate: The DP shall have the right to nominate an individual who upon DP's death can exercise the DP's rights under the DPDPA.

**DPDP Rules**: Under the DPDP Rules, in order to enable the DP's to exercise the aforementioned rights, it is required that DF's/Consent Managers publish on their websites the means by which such rights shall be exercised, any particulars such as a specific username/user ID required to identify DP for the exercise of its rights.

**Implications for lenders**: The borrower's right to withdraw their consent, would be very pertinent for lenders to understand, and natural question arises as to what are the outer boundaries of this right. In our view, the right to withdraw consent accrues where consent is the basis for processing personal data. Where however, consent is not the basis of processing personal data, and data processing is pursuant to legitimate use, then there would be no grounds to withdraw consent, save and except to the extent where the consent towards processing of personal data has been voluntarily provided under Section 7(a) of the DPDPA[1]

For example: Where the data is being processed for other purposes (such as to generate borrower analytics, cross-sell/cross-market products), then because consent might have to be the basis for processing the data, the borrower would also have a right to withdraw the consent.

This is co-extensive with the obligations placed upon lenders under Para 10.2 of the DL Guidelines, which require that the borrower shall be provided with an option to give or deny consent for use of specific data, restrict disclosures to third-parties, and even revoke consent already given. However, the DPDP Rules not only prescribe the "what", but also the "how". Thus, compliance burden would not be discharged merely by providing a clause in the loan documents to the effect that borrower may withdraw consent, now lenders would also need to publish how the borrowers may do so.

[1] Reference may be made to Section 11(1) of the DPDPA.

**Other factors/implications**: In respect grievances or queries raised regarding lender functions, the law typically prescribes specific time frames within which such concerns must be addressed. For instance, the Consumer Protection Act mandates that customer grievances be resolved within 30 days, and RBI regulations similarly require borrower grievances to be addressed within 30 days. A similar approach is captured under Section 13(2) of the DPDPA, which suggests that grievances raised by borrowers be addressed within a prescribed period.

Neither Rule 9 nor Rule 13(3) of the DPDP Rules governing grievance redressal specify a timeline for resolving grievances related to the processing of personal data. Similarly, Rule 7(e) does not mandate a specific timeline for addressing queries raised by the DP in the event of a data breach. While the language of Rule 13(3) may imply that the DF has discretion in determining the timeframe for grievance resolution, this discretion must be exercised fairly and responsibly, particularly when dealing with borrowers.

The absence of explicit timelines in the DPDP Rules should not be interpreted as granting lenders unrestricted latitude in addressing grievances. Lenders must act in good faith, ensuring fairness in all their dealings with borrowers. Additionally, lenders are bound by their banker's duty of confidentiality, requiring them to maintain the secrecy of a borrower's affairs and details. Grievances related to personal data raised by borrowers would fall within the scope of this confidentiality obligation and, in our view, should be resolved within 30 days of receipt.

While lenders may adopt shorter timelines for grievance resolution under the framework of the DPDPA and the DPDP Rules, however, they must ensure that no grievance remains unresolved beyond the 30-day period. If grievances are not addressed within this stipulated timeframe, borrowers have two recourse mechanisms: they may approach the RBI Ombudsman and/or escalate the matter to the DPB.

**Penalties**: Penalties for the same may extend to ₹50 crore.

## 7. Additional obligations of a Significant Data Fiduciary (Significant DF) - Rule 12

**DPDPA Context:** Section 10 of the DPDPA introduced the Concept of a Significant DF. Section 10 of the DPDPA establishes additional responsibilities on such Significant DF like that of appointment of a Data Protection Auditor, carrying out periodic Data Protection Impact Assessment via an independent auditor etc. The entities to be considered a Significant DF will be notified by the Central Government.

**DPDP Rules:** Rule 12 of the DPDP Rules, titled "Additional Obligations of Significant DF," does not impose many additional responsibilities. Instead, it primarily focuses on the periodicity of conducting Data Protection Impact Assessments (DPIAs). It also mandates that the data auditor conducting the DPIA must report any significant or material observations to the Data Protection Board (DPB). As per the DPDP Rules the following obligations need to be ensured by the significant DP:

a. Conduct DPIA once in every 12 months

b. Ensure that the data auditor who conducts the DPDIA furnishes the DPB significant observations in relation to such DPIA;
c. Conduct DD to verify the algorithmic software deployed by it for the processing of personal data is not likely to pose a risk on the right of the DP
d. In case Central Government notifies towards processing of certain personal data, significant DF to undertake measures basis the recommendations the DF to also further ensure that such personal data is not transferred out of India

**Implication for Lenders:** In case the Lender is notified as a significant DF by the Central Government it would need to comply with the obligations as provided under the DPDPA and the DPDP Rules.

**Penalties**: Penalties for the same may extend to ₹150 crore .

## 8. Processing of data outside in India - Rule 14

**DPDPA Context:** Section 16(1) of the DPDPA stated that the Central Government may, by notification, restrict the transfer of personal data by a DF for processing to such country or territory outside India as may be so notified.

**DPDP Rules:** Rule 14 of the DPDP Rules governs the processing of personal data outside India. It states that the processing of personal data covered under the DPDPA will be subject to restrictions and compliance requirements as determined by the Central Government. However, the DPDP Rules do not currently specify these requirements or restrictions, leaving their definition and implementation to the discretion of the Central Government.

When the DPDPA was introduced, there was significant anticipation in the market regarding the potential creation of a "*negative list*" of countries by the Central Government. Under this approach, the transfer and processing of personal data would be prohibited in listed nations, while all other jurisdictions would be deemed compliant for processing personal data. As of now, we await clarity on the Central Government's approach and any standards or restrictions it may establish for processing personal data outside India.

**Implications for lenders:** For lenders engaged exclusively in digital lending, Paragraph 11.4 of the DL Guidelines strictly prohibit the storage of borrower data outside Indian jurisdiction. Even if the Central Government notifies the standards and requirements under Rule 14 of the DPDP Rules, borrower data must always adhere to the data localization requirements outlined in Paragraph 11.4.

In contrast, for physical lending, lenders may need to wait for further notifications from the Central Government to understand how these DPDP Rules will apply to them.

**Penalties**: Penalties for the same may extend to ₹50 crore.

**To Get in Touch with Us**