Authors: Subhojit Shome & Archisman Bhattacharjee
Email: finserv@vinodkothari.com
Date: July 05, 2024

Consent Managers for NBFCs

Implementation Challenges and Other Issues

Contents

1. Introduction

The Digital Personal Data Protection Act, 2023 (DPDP Act) was officially implemented through a gazette notification dated 11th August, 2023. This legislation focuses on the processing of digital personal data, encompassing data collected digitally or originally non-digital but subsequently digitised. The genesis of the DPDP Act can be traced back to the landmark Supreme Court judgement in *K.S. Puttaswamy v. Union of India*, commonly known as the Aadhaar judgement, which affirmed the right to privacy as a fundamental right under Article 21 of the Constitution of India.

A pivotal aspect of the DPDP Act is its stringent requirements for the processing of personal data, foremost among them being the necessity of consent[1]. In this regard the DPDP Act introduced the concepts of Data Principal, Data Fiduciary and Data Processor. In the context of NBFC lending, these concepts may be illustrated as below.

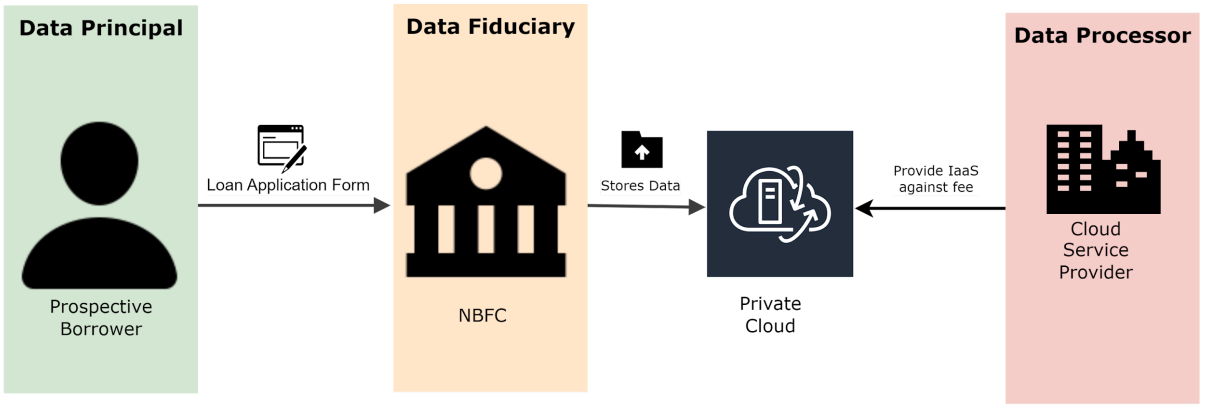

Figure 1: Data Principal, Data Fiduciary and Data Processor in the Course of NBFC Lending (Ref. our article - HERE)

Additionally, the DPDP Act introduces the innovative concept of Consent Managers, tasked with overseeing consent management on behalf of the Data Principal. Beyond consent, the DPDP Act delineates other grounds for processing personal data, including legitimate uses specified in Section 7, which do not mandate consent from the data principal for processing. The grounds of processing as has been provided by the DPDPA is as follows:

[1] As per Section 6 of the DPDPA "*The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose*"

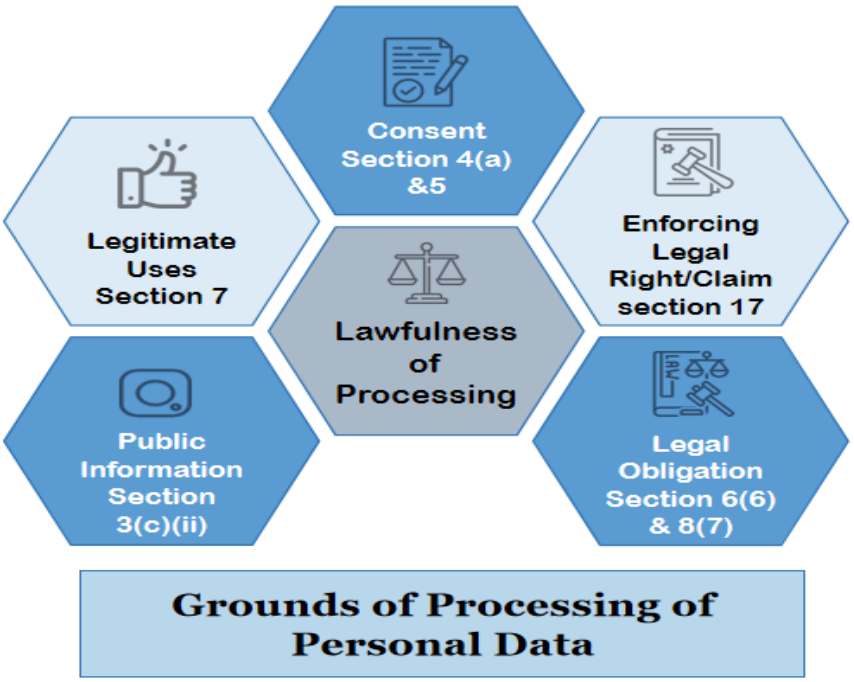

Figure 2: Legal Basis for Processing of Personal Data

However, for the purposes of this discussion, this article will focus on exploring the role & requirement of the consent manager, implementation of consent management and issues relating to consent management; especially when it comes to consent management for NBFCs.

2. Requirement of Consent manager

2.1. The DPDP Act mandates obtaining proper consent as essential for lawful personal data processing, with penalties starting at Rs. 50 crores for breaches.

2.2. A consent manager, defined in Section 2(g), acts as a registered intermediary facilitating individuals in giving, managing, reviewing, and withdrawing consent via a transparent platform. This role is specific to consent-based data processing, not legitimate uses.

2.3. According to para 6(8), the consent manager is directly accountable to the Data Principal (individual). Businesses, especially in digital lending, might benefit from integrating consent managers to ensure effective consent management. While consent managers streamline the process, the responsibility for compliance with DPDP Act standards remains with the Data Fiduciary. In light of the same, we have analysed below the relationship between Data Fiduciary and Consent Manager in circumstances where the data fiduciary has onboarded a Consent Manager:

a. Relationship between data fiduciary and consent manager

The Data Fiduciary as well as the consent manager are individually responsible for the personal data within their possession and accordingly, even if a consent manager has been

onboarded by a data fiduciary in our view the relationship between the data fiduciary as well as the consent manager shall at times be that of a principal to principal relationship and never can be a principal-agent relationship.

b. Liability of data fiduciary and consent manager

In our view, considering that the relationship of a Data Fiduciary with that of the Consent Manager is that of a principal to principal, the liability of the Data Fiduciary and the Consent Manager should be joint as well as several.

c. Is the consent manager a data fiduciary or a data processor?

According to the DPDP Act, a Data Fiduciary is defined as "*any person who, alone or with others, determines the purpose and means of processing personal data.*" Similarly, a Data Processor is defined as "*any person who processes personal data on behalf of a data fiduciary.*" In this context, a Data Processor is accountable to the Data Fiduciary for the processing activities carried out on personal data. Furthermore also drawing reference to sections 8(2)[2] and 8(5)[3] of the DPDP Act, it might be implied that the relationship between a Data Fiduciary and Data Processor is that of principal-agent since the liability for breach of personal data along with accountability of personal data rests with the Data Fiduciary.

However, under section 6(8) of the DPDP Act, a Consent Manager is explicitly accountable to the Data Principal. This raises the question: does this accountability exclude the possibility of a consent manager being accountable to the data fiduciary for its processing activities? Our answer to the same would be in the positive for the reasons as has been listed below:

i. As previously discussed, the relationship between a Data Fiduciary and a consent manager operates on a principal-to-principal basis. Aside from meeting performance metrics, periodic data reconciliation, and forwarding data subject requests as stipulated in the contract etc., the Consent Manager's primary accountability lies with the Data Principal under Section 6(8) of the DPDP Act. Therefore, in our perspective, the Consent Manager should not be held accountable to the Data Fiduciary for the processing it conducts on personal data.

ii. The processing of information by a Consent Manager is governed not by the purposes for which the Data Fiduciary obtained consent or on the direction of the data Fiduciary, but rather by the powers granted to the Consent Manager under Sections 2(g) and 6(7) of the DPDP Act. These provisions empower the Consent Manager to facilitate the Data Principal in giving, managing, reviewing, and withdrawing consent.

[2] Section 8(2) DPDP Act: *"A data fiduciary may engage, appoint, use or otherwise involve a data processor to process personal data on its behalf for any activity related to offering of goods or services to data principals only under a valid contract."*

[3] Section 8(5) DPDP Act: "*A data fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a data processor, by taking reasonable security safeguards to prevent personal data breach*"

iii. Grounds for processing personal data are determined by the Consent Manager. In our view processing of personal data by a Consent Manager can be done only to the extent by the Consent Manager to facilitate the Data Principal to give, manage, review and withdraw consent so provided by the Data Principal.

Hence having considered the above it cannot be stated that a Consent Manager processes personal data on behalf of a Data Fiduciary and should not in our view qualify as a Data Processor as per the definition provided under section 2(k) of the DPDP Act.

Furthermore, if a view is taken that a consent manager is a Data Processor who processes data on behalf of the Data Fiduciary, the same could potentially undermine the accountability to the Data Principal which is fundamental to the role of a Consent Manager.

d. Consent manager as an evaluator of the practices of the data fiduciary

Under section 6(8) of the DPDP Act, a Consent Manager is primarily responsible for facilitating the Data Principal to give, manage, review and withdraw their consent through an interoperable platform. When a data fiduciary engages a consent manager, we believe the consent manager assumes the crucial role of safeguarding the customer's consent from potential misuse by the data fiduciary.

The term "*review*" in the DPDP Act might suggest that the Consent Manager may also be tasked with monitoring whether the consent obtained by the data fiduciary is strictly adhered to for its intended purpose. This oversight implies reciprocal accountability, with the Data Fiduciary being answerable to the consent manager as well.

However, currently, from the DPDP Act, it is not certain whether a Consent Manager can act as a reviewer of the consent so provided to the data fiduciary and demand accountability from the Data Fiduciary, or its role would just be limited to an intermediary acting as a communication bridge/ messenger between the Data Fiduciary and Data Principal.

However, if we adopt the interpretation that a Consent Manager can act as a reviewer of consent on behalf of the Data Principal and demand accountability of processing from the data fiduciary, instead of merely allowing the Data Principal to view the consent that they have provided, such would create a system similar to a "maker and checker" model in managing personal data. This approach not only boosts accountability but also reinforces data protection under India's regulatory framework.

3. Whether onboarding of a consent manager is mandatory?

Reference is made to section 6(7) of the DPDP Act, which stipulates, "*The Data Principal **may** give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager*." The use of "*may*" indicates that Data Principals have the option to provide consent directly to Data Fiduciaries or via a Consent Manager.

Operationally, when consent is facilitated through a Consent Manager, it implies that the manager should have access to the privacy policy/ notice of the Data Fiduciary to fulfil the requirements outlined in section 5 of the DPDP Act. Additionally, for Data Principal to effectively review, manage, or withdraw their consent, there must be a clear communication channel between the Consent Manager and the Data Fiduciary. Furthermore this line of communication also needs to have a reasonable TAT so that the customer requests are also addressed within time, which seems more of a contractual obligation between a Consent Manager and a Data Fiduciary.

While the DPDP Act is designed to benefit Data Principals, it does not explicitly mandate the onboarding of a Consent Manager by a Data Fiduciary. Interpreting the Act in favour of Data Principals suggests that onboarding a Consent Manager could be advantageous. However, the issue still remains unclear.

4. Implementation of Consent Management

The following are some of the challenges in implementing consent management via a Consent Manager with regard to NBFCs -

4.1. NBFCs, especially digital lenders, are subject to consent requirements not merely via the DPDP Act but also through various regulations prescribed by the RBI. Such regulations require NBFCs, especially digital lenders, to obtain explicit and prior consent even where other lawful bases for processing are available to the Data Fiduciary. It is to be seen whether Consent Managers will also aid NBFC in obtaining RBI-related consent from its clients. In this regard, the following challenges exist -

a. While the DPDP Act restricts itself to processing **personal** data the RBI requires consent for "*any **collection of data***" from the user,

b. The RBI also mandates that **access to user's phone resources** (camera, microphone), etc. is taken only after obtaining user consent.

4.2. There is a question as to whether consent at every instance of obtaining personal data is necessary. In this regard we may examine the illustration provided under section 5(1) -

X opts for processing of her personal data by Y in a live, video-based customer identification process. Y shall accompany or precede the request for the personal data with notice to X, describing the personal data and the purpose of its processing.

A view may be taken that once consent is taken along with due notice, as per section 5(1), X may be subjected to multiple iterations of the V-CIP process[4] as long as the data being processed during the sessions is the same. An alternative view may be every V-CIP session must be consented to and preceded or accompanied by the notice.

4.3. When it comes to umbrella consent the guideline of the RBI is clear -

[4] It is to be noted that the requirement to obtain consent, under the DPDP Act, for the purposes of performing V-CIP as part of the KYC process, a legal obligation upon the NBFC, a regulated entity, is in itself questionable.

*A **one-time access** can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/ KYC requirements only, with the explicit consent of the borrower.*

The mention of the term "one-time" makes it clear that any repeat access will require fresh consent from the user.

4.4. The DPDP Act specifies the need for free, specific, informed, unconditional and unambiguous consent with clear affirmative action, with the onus of proving consent has been received put upon the data fiduciary. Similar are the requirements of the RBI that talk about consent being explicit, prior, informed, and auditable. This rules out the possibility of obtaining any post-facto consent via any loan documentation or addendum thereto.

4.5. The question of whether consent, under the DPDP Act, may be taken by use of a comprehensive privacy agreement/ policy packaged within a clickwrap may also have a negative response. The answer will depend on the view taken under para 4.2. and Consent Managers will need certainty from the rule-making body whether an umbrella privacy policy-based consent will suffice.

4.6. There is a question as to whether the Consent Manager will also have to track the services the Data Principal subscribes to from a particular NBFC/ services provider. It becomes essential to do this if one goes by the illustration provided under section 6(6) where opting in or opting out of a service (intimations via app instead of via email) dictates the personal data that may be processed (the need for processing email id of the data principal becomes redundant).

4.7. Verifying identity - NBFCs have stringent PMLA/ KYC requirements to verify customer identity, perform dedup and assign a single unique identifier (UCIC) to the customer. For the purposes of obtaining consent as well the identity of the person providing such consent will need to be established. In all likelihood, the consent manager will also have to devise a method to establish the identity of data principal. It is to be seen whether the dedup process is outsourced by the NBFCs to the consent manager and whether adoption of a common identifier takes place.

4.8. The communication process among the data principal, consent manager and data fiduciary will have to be bi-directional. This is not only the case for grievance redressal but also for consent management. For example, consider the case where the data principal has withdrawn consent for processing their personal data or has requested its deletion. The consent manager under the DPDP is required to convey the same to the data fiduciary, however, if the data fiduciary cites a valid reason for non-deletion of data the same would also be required to be communicated by the consent manager to the data principal.

5. Issues

The possible issues with having a separate consent manager framework are as below:

a. Consent managers may profitably extend their roles as KYC, application collection and document execution platforms as well. Conversely, entities performing such allied services may provide consent management services. The consent managers may start acting as an NBFC's digital lending application (DLA) and conflict of interest issues may arise.

b. While the consent manager is expected to act at the behest and in the interest of the data principal, it is expected that its income will be largely derived from the data fiduciary. Can we not expect that he who pays the piper will also call the tune?

c. Will compliance management and consent management be integrated or will consent managers be relegated to merely collecting and managing consent information? With the two processes disjointed the possibility of a gap between what was consented to and what is being processed, and how, may arise.

d. This raises the corollary question - who will flag the non-compliance? Will it be done through regular inspections and audits performed by the DPB or based on complaints raised by the data principal? The sheer number of data fiduciaries and the opaqueness of data processing, respectively, make it difficult for both these parties to act as effective monitoring agencies. consent managers may be an answer.

e. Section 13 of the DPDP casts an obligation upon both the consent manager as well as the data fiduciary to address grievances raised by a data principal. The Rules now need to set the individual responsibilities of the consent manager and data fiduciary when it comes to correcting errors and omissions. Further, it would be beneficial to have a joint responsibility framework for grievance redressal between the data fiduciary and consent manager. This may be on the lines of what the RBI has prescribed for credit bureaus and credit institutions.[5]

6. Conclusion

Consent managers may be another candidate for public infrastructure on the lines of the ONDC. Technical, operational, financial, and other conditions may then be prescribed not merely by regulation but also by code and permitted platform behaviour. With the consent manager, itself, holding a large amount of 'marketable' data and having a direct interface with the public it is likely that such entities will find themselves outside the regulatory 'Lakshman Rekha' drawn by the Government/ Data Protection Board. The market has already started to witness entities advertising themselves as consent managers and the sooner the Government frames the rulebook for these entities, the better.

[5] Ref. RBI Circular on Framework for compensation to customers for delayed updation/ rectification of credit information dated October 26, 2023.