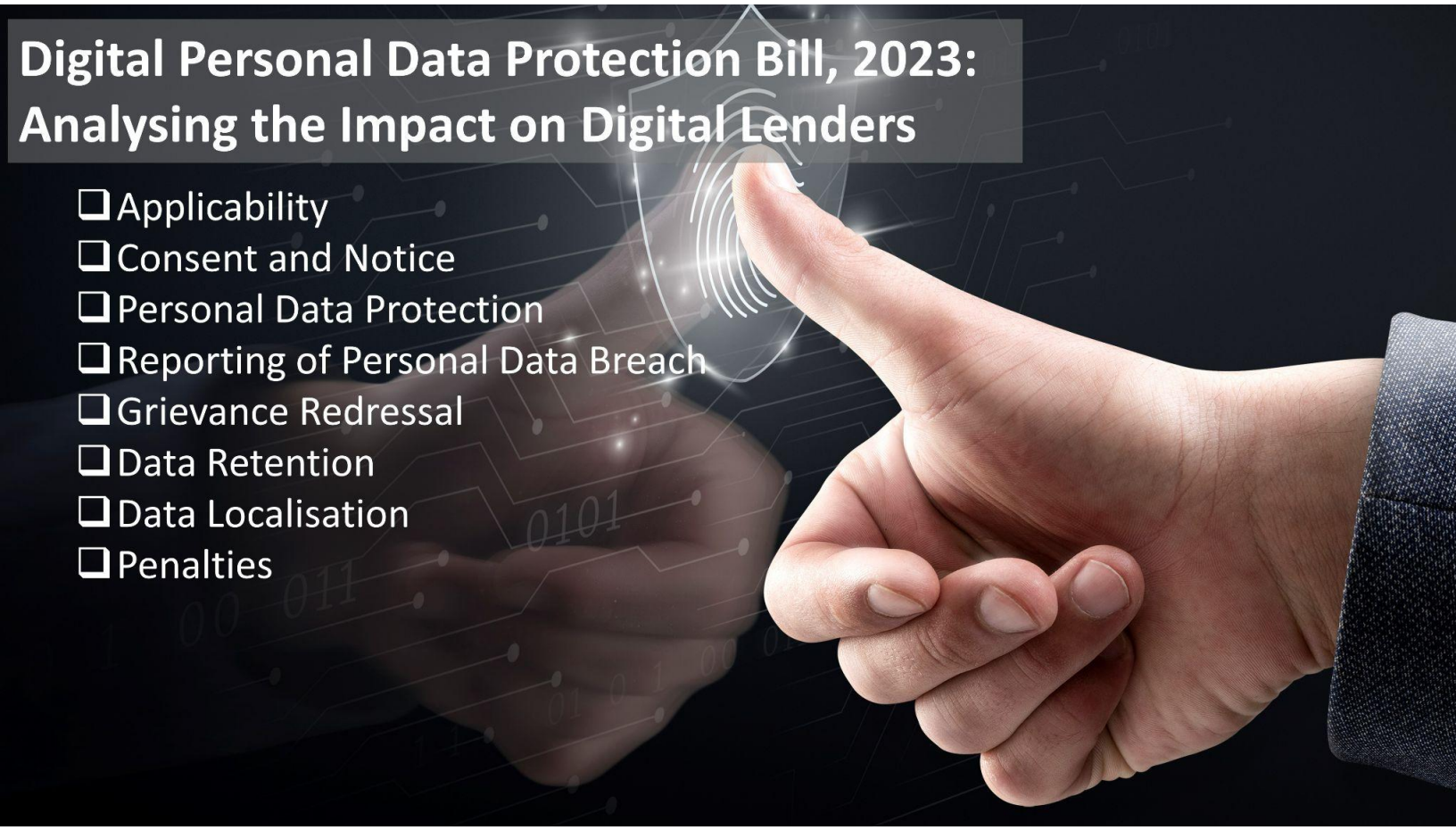
Digital Personal Data Protection Bill 2023: Analysing the Impact on Digital Lenders

Author: Subhojit Shome, Team Finserv
Email: subhojit@vinodkothari.com

Date: August 08, 2023



Background

The Ministry of Electronics and Information Technology (MeitY) introduced a revised draft of the Digital Personal Data Protection Bill, 2022 ('2022 Bill') on November 18, 2022 for public comments and has subsequently redrafted this 2022 Bill and introduced it as Digital Personal Data Protection Bill, 2023 ('Bill') in the Lower House of the Parliament on August 03, 2023[1]. The Bill, as was its earlier version, is intended to be technology and sector-agnostic and, hence, shall serve as a broad guide for digital data protection across all sectors.

[1] The Lower House of the Parliament (the Lok Sabha) has passed this Bill on August 07, 2023 and now it is due to be tabled in the Rajya Sabha.

We had earlier provided an analysis of the 2002 Bill; in this write-up we present the broad prescriptions of the 2023 Bill on the Lendingtech sector, including NBFCs engaged in digital lending.

Contents

Abbreviations Used

Board/ DPBI	Data Protection Board of India
CDD	Customer Due Diligence (as provided in the Know Your Customer Direction)
DF	Data Fiduciary
DL	Digital Lending (as defined in the DL Guidelines)

DLA	Digital Lending Application (as defined in the DL Guidelines)
DP	Data Processor
DPL	Data Principal
DPO	Data Protection Officer
KYC	Know Your Customer (as provided in the Know Your Customer Direction)
RE	Regulated Entity (as defined in the DL Guidelines)
SDF	Significant Data Fiduciary
TDSAT/ Appellate Authority	Telecom Disputes Settlement and Appellate Tribunal

Highlights of the Bill

Applicability

Unless explicitly excluded by rules, digital lenders and NBFCs, in general, will get covered under the ambit of the proposed Act, as information shared by customers/ borrowers of such entities will involve "Personal Data". Actions of lenders amounting to "processing" (which is, indeed, quite wide) will come under this law.

See Applicability section

Consent

Importantly, the Bill mandates an explicit and informed consent from the Data Principal, subject to a carve-out for "legitimate uses", which is regarded as 'deemed consent'.
The effect of this requirement on digital lenders who are already complying with the DL Guidelines issued by the RBI may be minimal.

See Explicit and Deemed Consent section

Notice

Data Fiduciaries to provide prior notice to Data Principals for all cases where data processing requires consent of the Principal.
In case notice has been provided/ content taken before the commencement of the proposed Act, the Fiduciary is required to reissue the notice in conformity of the Act, where the same is lacking.
Requirements for fresh notice may not be applicable for digital lenders or NBFCs, in general.

See Requirement of Fresh Notice section

Figure 1: Highlight - Applicability, Consent and Notice

Data Protection Measures

The Bill provides for periodic Data Protection Impact Assessment/ audit, for "significant data fiduciary", however, it is light in providing any specific cybersecurity measures. See sub-sections (4) and (5) of section 8.
Information/ cybersecurity requirements as currently provided in terms of section 43A of the Information Technology Act, 2002 to get overridden.
NBFCs have specific guidelines, including under the Master Direction - Information Technology Framework for the NBFC Sector, which are stricter and more specific. These will continue to apply.

See Sensitive Personal Data & Information (SPDI) section

Reporting Data Breach

The Bill requires DFs to provide notice of data breaches to the Board that will be established under this proposed Act and also to every DP whose personal data is affected by such breach.

NBFCs are already required to report certain cybersecurity incidents to the RBI and also to CERT-In (as provided under the IT Cert-In Rules). Once the Bill becomes effective, NBFCs will have this additional reporting responsibility when it comes to information/ cybersecurity breaches.

See Reporting Personal Data Breach section

Grievance Redressal Mechanism/ Data Protection Officer

Data Fiduciaries to have grievance redressal mechanism for any complaints from Principals under the law. Significant Data Fiduciaries to also appoint a DPO; unaddressed grievance may be escalated to the Board.
DL Guidelines also require the implementation of a grievance redressal framework by digital lenders and NBFCs, in general, are covered under the ambit of the internal ombudsman/ integrated ombudsman based on certain functional/ threshold criteria and hence, they may not be majorly affected by the Bill, however, they may have to institute an additional grievance redressal channel with the Board as the escalation authority.

See Grievance Redressal and Escalation sections

Figure 2: Highlight - Data Protection, Reporting of Data Breach and Grievance Redressal

Personal Data Retention

The Bill allows personal data to be retained by the DF or its authorised DP, till a "reasonable period" post completion of the specified purpose or from withdrawal of consent by the DPL to store/ process such data, whichever is earlier.
The Bill, however, allows the DF to retain personal data for a longer period if any law so requires. NBFCs, including digital lenders, are required to retain records under KYC/ PMLA obligations.

See Personal Data Retention and Right to Forget sections

Data Localisation

The Bill does not impose any data localisation requirement on the DFs, however, it confers on the Central Government the authority to restrict, by notification, transfer of personal data by a DF for processing to such country/ territory outside India as notified.

This provision allays concerns of several parties, including big tech, about the extent of data localisation that will be imposed. When it comes to digital lenders, however, the RBI's prescription to store customer/ borrower data in servers located within India is quite clear.

See Data Localisation section

Penalties by the ton

For various breaches on the part of the DF the schedule under section 33(1) of the Bill specifies penalties ranging from ₹50 crores to ₹250 crores (failure in taking sufficient security safeguards to prevent personal data breach).

See Quantum of Penalty section

Figure 3: Highlight - Data Retention, Localisation and Penalties

Significant Provisions

While certain laws, like the Information Technology Act provided for data protection norms for certain types of data; the current Bill, once enacted into law, is going to be first of its kind, in India, that specifically deals with the privacy rights of Indian citizens and will have an overarching ambit over multiple sectors and commercial practices. With regard to the NBFC/ digital lending sector specifically, we were able to identify the following critical provisions -

Applicability

Section 3 of the Bill states that the proposed Act applies to -

> *[the] processing of digital personal data within the territory of India where the personal data is collected—*
> *(i) in digital form; or*
> *(ii) in non-digital form and digitised subsequently*

Hence, the proposed Act will cover not only instances of digital lending where borrower information is collected and processed using digital means but also traditional lending practices where personal data may be collected physically (say, a borrower provides information using a physical loan application form) and is subsequently digitised and processed.

The definition of "processing" sufficiently wide to include any form of action on data including storage and covers both wholly automated and partly-automated processing. The 2022 version of the Bill had only spoken of *"automated operation or set of operations"* when defining the term processing.

In this context, the concepts of data fiduciary (DF), data processor (DP) and data principal (DPL) as introduced by the Act needs to be discussed. Taking the last concept mentioned first, DPL is the individual/ natural person to whom the personal data pertains to, DF is the entity that determines the purpose and the means for processing the personal data pertaining to the DPL and the DP is the entity that processes the data on behalf of the DF.

In the context of lending by NBFCs, the DPL, DF and DP are identified in figure 4.

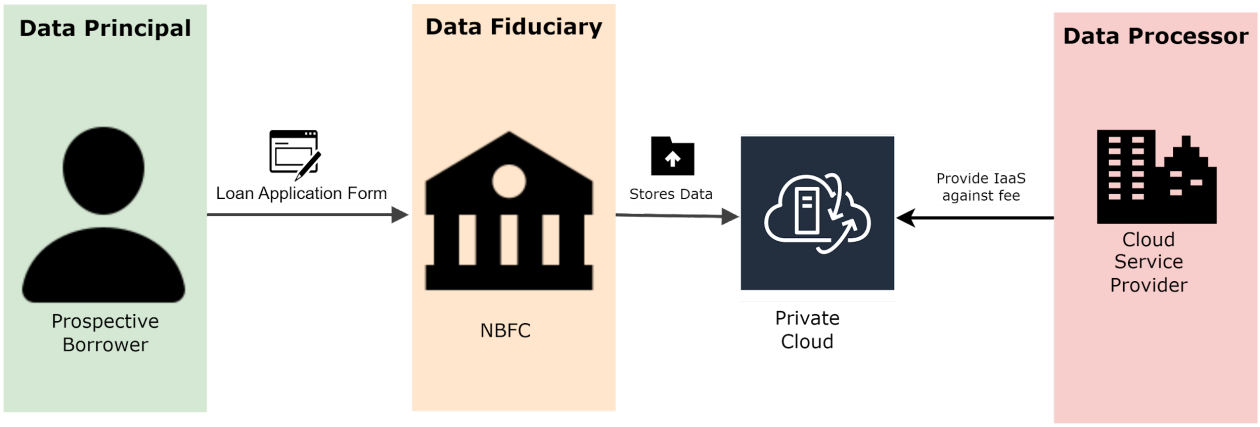


Figure 4: Data Principal, Data Fiduciary and Data Processor in the Course of NBFC Lending

Explicit and Deemed Consent

As was provided in the 2022 iteration of the Bill, the Bill allows processing of personal data of a DPL only under the following situations

a. Where the DP has provided her consent (**explicit consent**)
b. For certain legitimate uses (**deemed consent**)

When it comes to the first situation, as per section 6 of the Bill, consent provided by the DPL

> *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*

In the case of deemed consent, *"certain legitimate uses"* are listed under section 7 of the Bill. The following "legitimate use" case is pertinent for digital lenders -

> *(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data.*

Do note, that the meaning of the term "specified purpose" used here is not the same as that provided in the interpretation clause wherein "specified purpose" is defined as -

> *"specified purpose" means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder*

This is because in the case of "deemed consent" the question of providing a "notice" (as discussed under the 'Requirement of fresh notice' heading) does not arise. Hence, one must construe the term "specified purpose" here in relation to the DPL, i.e., the purpose for which the DPL has approached the DF.

Lets assume a prospective borrower applies for an unsecured personal loan by filling in an e-application form using the lender's DLA. The lender may process the personal data voluntarily provided by such individual for the purposes of, say, KYC/ CDD, credit appraisal, sanction, disbursement, servicing and such other activities required to required for the purposes of the unsecured personal loan, however, the lender cannot use such personal information for cross-selling or marketing of new products and services as these are not the purpose for which the borrower has voluntarily provided her personal data.

When it comes to digital lending by regulated entities (RE), the DL Guidelines, however, only allow access and sharing of data subject to 'prior and explicit consent' of the prospective borrower and the purpose for which data is being collected/ shared has to be explicitly informed to the prospective borrower, even if the data is being voluntarily offered by such borrower or personal data processing is necessitated by the nature of the transaction itself (say, performing KYC). Hence, the DL Guidelines pose a stricter requirement on the RE involved in digital lending when it comes to the requirement of consent.

Requirement of Fresh Notice

Section 5 of the Bill requires the Data Fiduciary (DF) to provide notice to the Data Principal (DPL) before taking consent to process the personal information of the DPL. The notice needs to contain information about the personal data that is being collected, the rights of the DPL under the Bill and the manner in which the DPL may make a complaint to the Board.

Sub-section (2) of section 5 goes on to mandate that where the DF had received consent prior to commencement of the Act, it will need to reissue a notice to the DPLs containing the aforementioned information.

Regulation 10 of the DL Guidelines also requires digital lenders to obtain prior, informed and explicit consent from the borrower/ prospective borrower when it comes to collecting, processing, retaining and sharing personal data with third parties. Additionally, the Bill also mandates that the DF provide the DP the option of receiving the notice in English or in any of the languages specified in the 8th Schedule of the Constitution. Hence, lenders will have to make appropriate changes to their digital lending apps (DLA) so as to allow its users to select the preferred language.

Once the DPDP Act comes into effect, digital lenders may also have to amend and reissue notices in conformity with section 5 of the Bill. Do note, however, that the Bill provides for both consent-based and "deemed consent-based" processing of personal data and the requirement of a notice does not arise in the latter case ,hence, it follows that the requirement of a fresh notice also does not arise in such a case.

Auditable Notice and Consent

Sub-section (10) of section (6) states -

> *Where a consent given by the Data Principal is the basis of processing of personal data and a question arises in this regard in a proceeding, the Data Fiduciary shall be obliged to prove that a notice was given by her to the Data Principal and consent was given by such Data Principal to the Data Fiduciary in accordance with the provisions of this Act and the rules made thereunder.*

This effectively means that the DF has to maintain an adequate audit trail of the service of notice and of the consent received/ withdrawn from/by the DPL. This mandate is in line with what the Digital Lending Guidelines require of the DLAs. We had discussed the need for digital lenders to obtain informed consent and maintain an audit trail in our FAQs on Digital Lending.

Withdrawal of Consent

The Bill also provides DPLs the right to withdraw consent already provided. Withdrawal of such consent triggers requirements to stop processing the DPL's personal data both by the DF and any DP authorised by the DF to process such data. Exception is allowed where retention is required or authorised under the provisions of the Bill/ Rules made thereunder (say need to maintain audit trail of consent - ref. Auditable Notice and Consent) or any other law for the time being in force in India.

The DL Guidelines have a similar provision where the borrower has to be mandatorily provided with an option to revoke and withdraw consent and digital lenders are reasonably expected to have implemented this prescription -

> *The borrower shall be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the app delete/ forget the data. [DL Guidelines - Para 10.2]*

It is, however, unclear as to whether the facility to withdraw consent implemented by the digital lenders satisfies the condition that the "*ease of [withdrawing consent is] comparable to the ease with which such consent was given".* Say for instance consent is provided in the form of clickwrap agreement wherein the borrower ticks an 'I Agree' box at the bottom of lender's privacy policy to indicate her consent, will it be reasonable for the lender to ask the borrower to email/ SMS the Company's GRO to withdraw such consent.

Withdrawal of consent also places upon the DF and DP data retention/ erasure requirements discussed under the 'Personal Data Retention' heading and bring with it similar issues when it comes to retention and processing of personal data to protect the interest of the DFs. The DL Guidelines had not spelled out the consequences of the revocation or withdrawal of consent on the relationship between the lender and borrower. The Bill, however, lends clarity to this by stating that the effect of such withdrawal shall be borne by the DPL, i.e., the borrower. There is, however, the question of whether the lender (DF) or its authorised third party service provider (DP) can continue to process personal data for the specific purposes of a subsisting relationship, say a live loan agreement, when it comes to a withdrawal of consent/ request to erase data by the borrower.

Specified purpose

Sub-section (1) of section (6) of the Bill states -

> *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.*

This clause is among the major substantive provisions in the Bill. One must note that this clause not only brings up the issue of consent but also the concept of "specified purpose". Specified purpose has been defined under section 2(za) as -

> *… the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder*

Using the same hypothetical case referred to under the "Explicit Consent and Deemed Consent" heading, in order to send promotional material regarding products and services offered by the lender, currently or in the future, to a prospective borrower who has approached the lender merely for the purposes of availing an unsecured persona loan, the lender will have to obtain explicit consent of such borrower by providing such notice as mandated under section 5(1) of the Bill.

Now, let's consider another case where as part of the loan application for an unsecured personal loan, the DLA also collects consent from the borrower to share her personal information with an insurance company for the purposes of insuring the borrower. Insuring the borrower is a common business practice when it comes to sanctioning unsecured personal loans and protects the legitimate interest of the lender and the operation of section 6(1) may be overridden by the "certain legitimate uses" clauses as per section 4(1)(b) of the Bill.

Personal Data Retention

Sub-section (7) of section 8 mandates -

> *A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—*
> *(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier;*

In the case of NBFCs, retention of personal data may extend well beyond the point when specified purpose is fulfilled due to operation of various laws (like the PMLA 2002) and RBI Guidelines, say for instance, a subsisting loan arrangement is fully serviced and the loan is closed, however, the NBFC is bound under the KYC Master Directions issued by the RBI to "maintain all necessary records of

transactions between the RE [Regulated Entity, i.e., the NBFC] and the customer, both domestic and international, for at least five years from the date of transaction". Hence, retention of personal data as part of such a regulatory mandate shall not be affected by the operation of the said clause.

There are cases, however, NBFCs retain information as prudent business practice although such retention is not explicitly mandated by any law or regulation. Say for instance, an NBFC retaining rejected loan application data for the purposes of pre-empting any regulatory challenges or civil litigation on the grounds of discrimination. In such a case, as is apparent, the specified purpose (obtaining a loan) is well over, in fact it did not even effectively begin and there is no legal mandate to retain such data. One can, however, appreciate the pragmatism of such a practice. Now, the question arises as to whether such retention will fall foul of section 8(7).

Section 8(7) states that the specified purpose shall be deemed to be no longer served when the DPL does not approach the DF, for performance of the specified purpose or to exercise any of her rights in relation to the processing of the personal data provided, for *"such time period as may be prescribed"*. We will have to wait to see whether the prescribed time period is reasonable when it comes to protecting the legitimate interests of the NBFCs and whether it is tied to the period of limitation when it comes to lodging complaints with the regulators or filing suits in the civil courts.

Another enabling clause is section 17 of the Bill where it allows "*the processing of personal data [when it] is necessary for enforcing any legal right or claim", however, this section goes on to explicitly mention the scenario of a "default in payment of a loan or advance" when it comes to non-applicability of the consent/ withdrawal of consent and "end of specified purpose" clauses.*

Right to Forget

Sub-section (3) of section 12 states -

> *A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.*

This clause is also on similar lines as the data retention requirements posed by the DL Guidelines and digital lenders are reasonably expected to have already put in place a framework for implementing such requirements. The Bill provides an additional right to the DPL to nominate a person to exercise those rights that are available to the DPL under this Bill in the event of the death or incapacity of such DP. Digital lender will have to incorporate such a nomination requirement on its DLA/ loan application form.

Reporting Personal Data Breach

The RBI's Master Direction on Information Technology Framework for NBFCs requires them to report *"all types of unusual security incidents"* as specified in the Annex-I to such directions to the RBI.

As per the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, entities are also mandatorily required to report certain cybersecurity incidents to the CERT-In.

Now, once the Bill becomes law, NBFCs (including digital lenders) will also have to report data breaches to the Board established under the proposed Act and also inform every DP (borrower/ other customer) whose personal data is involved in such breach.

Grievance redressal

The Bill requires DFs to institute effective grievance redressal mechanisms arising out of the provisions of the Bill as well as the rights of the DPL. The Bill proposes the requirement of having a data protection officer (DPO) by "Significant Data Fiduciaries" (SDF) to address any query/ complaint, raised in pursuance of the rights/ obligations under the proposed Act, on behalf of the DF.

The RBI's DL Guidelines also require digital lenders to have in place a grievance redressal mechanism to address complaints raised by it borrowers/ customer both with regard to it own activities as well as those arising from the activities of its lending service providers (LSP) including designating a grievance redressal officer (GRO). This prescription of the RBI puts a broader and stricter responsibility on the shoulders of the digital lender compared to the grievance redressal proposed in the Bill and the GRO designated by the digital lenders may also be given the duties of the DPO in case such lender is categorised as an SDF or falls in the category of entities designated as SDF. Such a digital lender, however, should have the DPO designated by its Board and ensure that the DPO has access to the Board/ Board Committees.

Escalation

In case, a grievance raised under the proposed Act or rules framed thereunder remains unattended or is not adequately resolved by the DFL, the DPL may escalate such a grievance to the Board for resolution.

Oversight of grievance redressal of NBFCs are provided for under the internal ombudsman/ integrated ombudsman scheme of the RBI. Under which grievance redressal mechanism of the RBI the NBFC will fall under depends on the scale (asset size) and/ or the type of activity (deposit taking) undertaken by the NBFC. In the case of digital lending, borrowers can escalate their grievances to the RBI using its CMS portal. Once, the Board, as provided in the Bill, becomes operational NBFCs will have to monitor and address an additional grievance escalation channel.

Data Localisation

As mentioned in the Highlights, The Bill does not impose any data localisation requirement on the DFs, however, it confers on the Central Government the authority to restrict, by notification, transfer of personal data by a DF for processing to such country/ territory outside India as notified.

This provision allays concerns of several parties, including big tech, about the extent of data localisation that will be imposed. When it comes to digital lenders, however, the RBI's prescription to store customer/ borrower data in servers located within India is quite clear.

Quantum of Penalty

The Bill in its Schedule specifies penalty amounts upwards of ₹200 crores on certain types of contraventions by DFs and has some of the highest penalties compared to that specified under any other law in effect. According to an RBI Report, the aggregate quantum of penalty in FY22 on banks and non-banking finance companies (NBFCs) by the RBI amounted to ₹65.32 crores, with the number of penalties being about three times more than the number in the previous fiscal. When compared to such a statistic, the penalty amounts recommended in the Bill are staggering.

Sensitive Personal Data and Information (SPDI)

Section 43A of the Information Technology Act, 2000, and the Rules thereunder classified a subset of personal data (e.g. financial information such bank account details) as "SPDI" and prescribed stricter measure with regard to obtaining consent for its storage and processing as well as information/ cybersecurity measures that needed to be employed to safeguard such data.

The Current Bill does not make a distinction between personal data and SPDI. In fact, once the Bill gets enacted into law, section 43A gets repealed and the very concept of SPDI disappears from India's legal landscape. An important implication of this is that an aggrieved Data Principal would not have a specific recourse for being compensated for the loss/ breach of their personal data and would need to seek relief provided by common law/ contract law.

Appendix - A Comparative View of the Current Bill vis-à-vis the 2022 Bill

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
Applicability	Applicable on processing of digital personal data within the territory of India. The digital personal data for this purpose shall include the personal data that is obtained from an individual to whom the personal data relates, to be known as Data Principal, digitally or personal data obtained physically and then digitised. Further, it shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals, within the territory of India. Profiling is defined as '*any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal.*'	In the Bill 2023, the applicability depends on the processing of data instead of "profiling" as under the Bill 2022. The term "processing" in relation to personal data, means both a **wholly or partly** automated processing of personal data. Much like the 2022 Bill 2022, the current Bill talks about processing of personal data **within the territory of India** in digital form or in non-digital form, subsequently digitised, and processing of personal data **outside the territory of India** in connection with any activity related to offering of goods or services to Data Principals in India.	*The practice of transferring data abroad is common in the fintech industry where the fintech is a part of a foreign corporate group or uses the services of foreign tech companies to evaluate their customer's behavioural patterns. It is noteworthy here that the 2019 Bill on data protection barred sharing of information outside India, which could have resulted in a complete disruption in the fintech business models, which are largely data-driven.* *However, in the subsequent Bills the prohibition was removed, and the Central Government has been empowered to notify restrictions on the transfer of personal data by a Data Fiduciary for processing of such countries as may be notified.* *The 2023 Bill, however, also added a clause stating that these provisions will not impact any other law which provides for a higher degree of protection for or*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
			restriction of transfer of data outside India. *In the context of Digital Lending, the DL Guidelines provide that REs cannot share/ store customer information in servers located outside India. Importantly, fintechs offer financial products based on the outcomes of customer profiling, which in many cases is done at a group level/service provider level; usually outside India.*
Legitimate Use	A person may process personal data for which the Data Principal has given or **is deemed to have given** her consent in accordance: or with the provisions of this Act.	A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,— (a) for which the Data Principal has given her consent; or (b) for **certain legitimate uses.** The 2023 Bill replaces deemed consent with the "certain legitimate uses" clause.	*DL Guidelines require digital lenders to obtain explicit consent of the borrowers when it comes to collection, retention and sharing of data. The impact of this section may be minimal when it comes to Digital Lenders who are already complying with the DL Guidelines.*
Exclusions & Exemptions	It has been provided that the provisions of the Bill shall not be applicable to: 1) non-automated[2] processing of personal data; 2) offline personal data;	It has been provided that provisions of the Bill shall not be applicable to: 1) personal data processed by an individual for any personal or domestic purpose;	*Only certain activities of digital lenders (like, compliance with any enforcement action, sharing of information with MCA, CRILC or IU) will get covered under such exclusions.*

[2] *"automated" means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data;*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
	3) personal data processed by an individual for any personal or domestic purpose; and 4) personal data about an individual that is contained in a record that has been in existence for at least 100 years. One important exclusion is when the personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India. Hence, in cases where (a) the Data Principal does not belong to the Indian territory, (b) the data does not belong to the Indian territory and (c) the transaction is taking place outside the Indian territory; but the processing of data happens in India, the Bill shall not be applicable.	2) Personal data that is made or caused to be made publicly available by - a) the Data Principal to whom such personal data relates; or b) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.	
Data Protection Board	The Bill proposes setting up of a Data Protection Board ('Board') by the Central Government, which shall carry out the functions of ensuring compliance with provisions of the Bill. The Board has been entrusted with powers similar to the regulators.	In line with the previous version of the Bill, the current Bill also prescribes institution of the Board by the Central Government.	*The Bill essentially brings Fintechs and Regulated Entities engaged in digital transactions within the ambit of the Board. It is noteworthy that Lending Service Providers ('LSP') and Digital Lending Apps ('DLA') are outside the purview of the RBI, hence, the DL Guidelines has vested the RE with the*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
			duty to 'ensure' that the LSPs and DLAs deal with customer's personal data with utmost care of confidentiality as the RE is required to do. *However, DLAs and LSPs, along with REs engaged in digital transactions, would now be brought under the purview of the Data Protection Board of India. This calls for fintech entities to enhance the data security and align the customer data privacy policies with the existing laws and technological standards. This also brings for the question if it would result in overlapping jurisdiction of RBI and the Board in respect of data security compliances by REs.*
Defining Data Principal, Data Fiduciary, Data	The Bill defines these terms based on the rights of the party on the data. The owner of the data or to whom such personal data related is termed as Data Principal; The person who requires the data to be processed and shall utilise the data for a purpose is termed as Data Fiduciary and the entity which shall process the data on behalf of the Data Fiduciary is known as Data Processor.	The current Bill additionally includes "legal guardian" as Data Principal when it comes to personal data of a "child" or a "person with disability"	*Here it becomes crucial to determine whether an LSP shall be considered a Data Fiduciary or Data Processor. LSPs are defined under DL Guidelines as 'An agent of a Regulated Entity who carries out one or more of lender's functions or part thereof in customer acquisition, underwriting support, pricing support, servicing, monitoring, recovery of specific loan or loan portfolio on behalf of REs in*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
			conformity with extant outsourcing guidelines issued by the Reserve Bank.' *LSP is an "agent" acting "on behalf" of the RE, for the purpose of providing financial services of the RE. However, from the perspective of the Bill, the classification of LSP shall be based on the nature of services provided by such LSP or the role played by them. Hence, if the LSP is only processing the personal data on behalf of the RE and not processing/storing the same for providing any other services on its own, it may apparently be considered as a Data Processor and not subject to the more rigorous prescription applicable to Data Fiduciaries.* *On the other hand, one may argue, in Fintech models it is oft that the LSP who is the entity interacting with clients (providing the DLA[3] or other such public platform) and majorly collecting, storing or processing data from the customer directly and acting as an outsourced service provider to the RE on a*

[3] *Digital Lending Application (DLA) - Mobile and web-based applications with an user interface that facilitate digital lending services.*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
			principal-to-principal basis and utilisation of the data may be done by the LSP for its own purposes as well.[4] *Hence, the obligations applicable to a 'Data Fiduciary' should become equally applicable to an entity playing such a role.* *Nonetheless, the Bill as it stands places onus on the Data Fiduciaries to ensure that its provisions are also complied with by the Data Processors employed by them and this appears to be similar in lines to how the RBI's Digital Lending Guidelines are drawn to ensure compliance by LSPs.*
Obligations of Data Fiduciary	The Bill provides for the obligations of the Data Fiduciary, which broadly include the following: a. Data processing shall be done only for a lawful purpose for which the Data Principal has given or is deemed to have given her consent b. For requesting consent for processing the data, an itemised notice containing a description of	The current Bill also imposes obligations on the Data Fiduciary, on similar lines - a. The need to ensure completeness, accuracy and consistency of personal data when such data is used to make a decision that affects the Data Principal or when such data is disclosed to another Data Fiduciary b. To appoint Data Processors only under a valid contract	*Similar obligations are also placed upon digital lenders by the RBI, however, such lenders will be subject to additional reporting requirements in case of personal data breaches when the Bill gets enacted into law.*

[4] For a more detailed analysis of the relationship among LSPs and REs and the obligations arising out it, refer to our article here - https://vinodkothari.com/2022/10/lending-service-providers-for-digital-lenders-distinguishing-agency-contracts-and-principal-to-principal-contracts/

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
	personal data sought to be collected and the purpose of processing shall be provided. Here, providing an itemised list would mean listing down the nature of data, and the purpose of processing the same. c. Report to the Board in case of a personal data breach. *Reporting of cybersecurity incidents to CERT-In is already mandated under the IT Act and Rules[5] and FinTechs registered as NBFCs with RBI are also required to inform the RBI on occurrence of cybersecurity incidents .*	c. Implement appropriate technical and organisational measure to ensure adherence to the proposed Act/ rules made thereunder, and 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 d. Reporting of data breaches to the Board and to every Data Principal affected e. Certain duties with regard to retention/ erasure of data	
Processing of personal data of children/ disabled person	The 2022 Bill required Data Fiduciaries to obtain verifiable parental consent of the parent/ legal guardian. It also prescribes certain other obligations (e.g. not undertake tracking or behavioural monitoring) on the Data Fiduciary when it comes to processing personal data pertaining to children.	The current Bill extends the consent requirement also to persons with disability and continues to prescribe additional obligations when it comes to processing personal data of children.	

[5] Ref. para 12(1) of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
Consent vs. Deemed Consent	The Bill recognises two kinds of consents that may be received from the Data Principal- (a) Explicit consent and (b) Deemed consent. Consent under section 7(1) of the Bill is defined as *any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose* Further, section 8 of the Bill recognises the circumstances which shall be deemed to be the consent of the Data Principal for processing of data.	As mentioned earlier, the current Bill replaces the concept of "deemed consent" with the "certain legitimate use" clause.	
Notice	On or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in clear and plain language. Fresh Notice - where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for	The current Bill continues to impose the obligation on the Data Fiduciary to serve notice to the Data Principal preceding or at the time of obtaining consent from the Data Principal. Also, where a Data Principal has given her consent for the processing of her personal data before the date of commencement of this Act,— (a) the Data Fiduciary shall, as soon as it is reasonably practicable, give to the Data Principal a notice informing her,— (i) the personal data and the purpose for which	*The requirement for fresh notice may not apply to digital lenders legitimately processing personal data voluntarily provided by the Data Principal for the specific purpose.*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
	which such personal data has been processed, as soon as it is reasonably practicable.	the same has been processed; (ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and (iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed The current Bill additionally requires the Data Fiduciary shall give the Data Principal the option to access the contents of the notice in English or any language specified in the Eighth Schedule to the Constitution.	
Withdrawal of Consent	Section 7(4) of the draft Bill allows the Data Principal to withdraw her consent subsequent to which, the Data Fiduciary should cease to process the personal data. The Bill explicitly provides that the *consequences of such withdrawal shall be borne by such Data Principal,* meaning thereby that the Data Fiduciary is well within its right to cease business transactions with the Data Principal. Further, under section 7(8) of the Bill, a Data Fiduciary is not entitled to refuse the services to Data Principal when the data Principal denies to give consent for the collection of additional personal data not necessary for the purpose of transaction.	The 2023 Bill retains most of what was provided in the previous version of the Bill, however, it excludes section 7(8) of the previous Bill.	*The DL Guidelines have a similar provision where the borrower has to be mandatorily provided with an option to revoke and withdraw consent. However, the DL Guidelines did not spell out the consequences of such revocation or withdrawal of consent, leaving some room for controversy as to whether the RE can end the transaction with the borrower or not. Now there seems to be clarity that the Data Fiduciary has the discretion to stop offering services to the borrower in the event the borrower revokes her consent, where such data is integral to the transaction. However, if there is a request for personal data that is not necessary for the purposes of the transaction in question the Data*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
			Fiduciary cannot cease service on denial or revocation of consent. Hence, the draft Bill defines the situation as to when the RE can refuse its services on grounds of denial/ withdrawal of consent by the borrower. This provision is significant as it highlights the need for collection of personal data to be justified in terms of the specific transaction it supports.
Auditable Consent	Section 7(9) of the Bill mandates that where the Data Principal's consent is necessary for processing her personal data and a question regarding this arises in any proceeding, the Data Fiduciary shall be under the obligation to prove that requisite notice was provided to the Data Principal for obtaining the personal data and the consent was duly obtained.	The current Bill carries the same provision	*This signifies that Data Fiduciaries have to keep an audit trail of the consent obtained. A similar provision finds place in the DL Guidelines where the REs have to ensure that the prior and explicit consent of the borrower obtained should have an audit trail.*
Significant Data Fiduciary (SDF)	The Bill introduces the concept of Significant Data Fiduciary (SDF). The Central Government shall notify entities or a class of entities as SDFs, based on factors such as volume and sensitivity of personal data processed, risk of harm to the Data Principal, potential impact on the sovereignty and integrity of India, etc. The major requirements prescribed for SDFs are:	The current Bill carries the same provision	*One may expect detailed guidelines for complying with the aforementioned requirements. The powers of the Central Government may also be delegated to the Board.* *In case regulated fintech entities are notified as SDFs, the question one may have is whether the GRO of such an*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
	• Appointment of a Data Protection Officer who shall be responsible for addressing the grievances of Data Principals; • Appointment of an Independent Data Auditor who shall evaluate the compliance of the SDF with provisions of the legislation based on the Bill; and • Undertake Data Protection Impact Assessment and periodic audit in relation to the objectives of this Act		*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.* *Also, in case the digital lender is undertaking IS Audit as mandated by the RBI Master Direction - Information Technology Framework for the NBFC sector, it should ensure provisions of this proposed Act are suitable incorporated therein.*
Right to Grievance Redressal	The Bill provides for the manner of redressal of grievances of a Data Principal. As per the Bill, every Data Fiduciary must have a grievance redressal mechanism to address the grievances of its Data Principals. The Data Principals may register their grievances with the Data Fiduciary in the manner provided in their grievance redressal mechanism. If the Data Principal is not satisfied with the response or when no response is received within 7 days, it can approach the Board.	The current Bill also provides for a grievance redressal mechanism on similar lines as the 2022 Bill. It, however, replaces the 7 days criterion for escalation to the Board with the following clause - *The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board.*	*DL Guidelines allow a borrower to lodge a complaint with the RBI Ombudsman if any grievances, including data related grievances, are not resolved by the RE within 30 days.* *The borrower would now have a dual recourse available to her - either to approach the RBI Ombudsman or the Data Protection Board. The borrower could lodge a complaint with the Data*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
			Protection Board if there is a personal data specific grievance.
Data Storage & Retention	Section 9(6) of the Bill provides that personal data cannot be retained by a Data Fiduciary when its retention is not necessary for legal and business purposes and when the purpose for which it was collected is no longer served. This particular provision hints towards strong discouragement for retaining the personal data longer than is necessary under law and for the entity's business. The Bill provides a "Right to correction and erasure of personal data" and on request for erasure of their personal data by the Data Principal, the Data Fiduciary is required to erase the such data that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose. The Bill also provides a Data Principal the right to nominate any individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights.	The current Bill also prescribes personal data retention provisions on similar lines.	Prevention of Money Laundering Act, 2002 and rules thereunder and RBI guidelines lay down the period for which the data and transaction records have to be mandatorily preserved by specified entities. Most customer-related data stored by digital lenders will fall under the ambit of such laws.
Disclosure to Data Principal	Section 12 imposes the obligation upon the Data Fiduciary to disclose a summary of the personal data processed by the Data Fiduciary and providing the identities of all	The current Bill provides Right to access information about personal data, on similar lines, to the Data Principal.	*FinTech companies collect personal data from a number of sources other than the Data Principal and also tend to share collected data with third parties, hence, it*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
	the Data Fiduciaries with whom personal data has been shared. The obligation of disclosure to the Data Principal is cast only upon the Data Fiduciary. The Data Processor, who is processing the personal data of the Data Principal, does not have an obligation to disclose under the Bill.		*may become a challenge to provide the said summary to the Data Principal. The timelines and scope of such summary that will be allowed to Data Fiduciaries for providing such data will be important in determining the sophistication of the system that they will have to put in place.*
Sensitive Personal Data	The Bill makes a stark departure from section 43A in as much as it does not provide for compensation to an individual whose data has been breached. Hence, by omitting section 43A, an aggrieved Data Principal would not have a specific recourse for being compensated for the loss of her personal data.	The current Bill also carries provisions to repeal section 43A once the Bill gets enacted into law.	
Appellate Tribunal	An appeal against any order of the Board shall lie to the High Court. Every appeal made under this section shall be preferred within a period of sixty days from the date of the order appealed against.	"Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997 Any person aggrieved by an order or direction made by the Board under this Act may prefer an appeal before the Appellate Tribunal. Every appeal under sub-section (1) shall be filed within a period of sixty days The appeal filed before the Appellate Tribunal under sub-section (1) shall be dealt with by it	*Digital lenders will need to cater to such additional channels of grievance escalation.*

Heading	2022 Bill	2023 Bill (Current Bill)	Impact on Digital Lenders
		as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date on which the appeal is presented to it.	