

INTERPLAY BETWEEN DATA PROTECTION AND DIGITAL LENDING

*Prepared by
The Digital Lenders Association of India*

In association with Khaitan & Co



**KHAITAN
& CO** ADVOCATES
SINCE 1911

TABLE OF CONTENTS

1. FOREWORD	4
2. EXECUTIVE SUMMARY	5
3. FINANCIAL INCLUSION THROUGH ACCESS TO CREDIT	7
4. ROLE OF DATA IN INCREASED ACCESS TO CREDIT	11
5. BROAD GUARDRAILS FOR PROCESSING OF FINANCIAL DATA	15
6. INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES	19
7. DLAI'S OBSERVATIONS ON THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022	26
8. CONCLUSION	29
9. CONTACT US	30

FOREWORD

As the FinTech industry continues to evolve and grow, it is important for industry leaders and members to stay informed and educated on the latest developments and trends. The Digital Lenders Association of India (DLAI) is committed to providing valuable insights and knowledge to our members and the industry at large through our Knowledge Committee's ongoing efforts to bring out whitepapers, podcasts, and webinars on important topics.

We are excited to present the latest whitepaper in this series, written by esteemed members of DLAI - Khaitan & Co and slice. The whitepaper, titled "Interplay Between Data Protection And Digital Lending," delves into the crucial topic of financial inclusion and the role of data in increasing access to credit. The whitepaper also addresses the important issue of data protection and the interplay between the Digital Personal Data Protection Bill and the Digital Lending Guidelines, as well as DLAI's observations on the Digital Personal Data Protection Bill.

We would like to extend our sincere appreciation and gratitude to the contributors of this whitepaper- Sanjay Khan Nagra, Smita Jha, Supratim Chakraborty, Prashanth Ramdas, Sumantra Bose, Pritish Mishra, Ishani Sahai, Anushri Uttarwar, Shramana Dwibedi, Tashi Gyane from Khaitan & Co, Bhawna Sangwan, Chief Legal and Strategy Office, slice for their hard work and dedication in bringing this valuable resource to our members and the industry.

DLAI Knowledge Committee

We invite all members and industry stakeholders to read and engage with this whitepaper as we continue to strive towards financial inclusion and responsible data practices in the digital lending industry.

EXECUTIVE SUMMARY

Digital lending in India is expected to grow into a USD 1.3 trillion market from a USD 270 billion market by 2030 according to some market estimates.¹ The growth brings with it an incredible opportunity to address the issue of inequitable access to credit in India.

On the other hand, data generation in India is expanding in volume on a yearly basis. With a large part of Indian population yet to transact online, access to data, especially financial data, is crucial to driving productivity, innovation and economic growth in India. The use of data in facilitating financial services and credit through usage of remote and automated technologies benefits all stakeholders including fintechs and the government in terms of productivity, innovation, and access to credit.

Data protection in India is currently regulated by MeitY and sectoral regulators prescribing standards for data security and data processing for various data. Recently, the government through an extensive consultation process released the draft of the Digital Personal Data Protection Bill, 2022 (DPDP Bill) which is one of the most simplistic and progressive data protection frameworks around the globe. The DPDP Bill is a great example of aligning the consumer's privacy rights with the anticipated innovations in digital technologies (including digital finance). The Reserve Bank of India (RBI) also provides for data security and data collection framework for each financial product regulated within its structure.

The next goal of digital financial inclusion in India should emphasis on facilitating appropriately timed, sized and priced financial products for the ever-increasing financial customers along with a

¹Inc42, "State of Indian Fintech Ecosystem Q3 2022" (2022). Available at <https://inc42.com/reports/state-of-indian-fintech-report-q3-2022/>.

EXECUTIVE SUMMARY

strong data protection framework to instil more trust and transparency in the fintech ecosystem. With the increase in the number of digital documents and API based tech stacks, DLAI is of the view that a uniform consent framework and broad guardrails determining the data processing standards for digital lenders would be a key enabler for achieving this goal. A uniform consent and privacy framework will ensure that the benefits of digital lending are experienced nationwide by harnessing the potential of innovative technologies.

India has laid the foundation for this expansion in digital lending through its Jan Dhan – Aadhaar – Mobile (JAM) trinity drive and has recently proposed the fourth version of India's data protection law. Further, the RBI notified the Digital Lending Guidelines last year which acknowledges the pivotal role played by data in the digital lending process and the need to process the same in a safe and sustainable manner.

This whitepaper outlines a regulatory framework, institutional architecture, and technological outline for data protection which can be adopted by the digital lending industry. The approach in the paper also stresses upon the need for accessibility of credit for the current population to improve their financial well-being.

For this reason, it has become crucial for the digital lending industry to focus on adapting from the global best practices in data handling and security centred on the principals of interoperability, privacy by design and a robust consent framework, as well as working with the Indian government and the RBI in enabling reflexive regulations to ensure that this upward movement does not stagnate nor turn exploitative.

FINANCIAL INCLUSION THROUGH ACCESS TO CREDIT

Financial inclusion has been a key objective of the Indian government and RBI. The Aadhaar framework laid the foundation of a publicly available interface in the form of IndiaStack which allowed financial institutions to utilise digital infrastructure to provide presence-less, paperless and cashless delivery of services.

The IndiaStack framework enabled the launch of Pradhan Mantri Jan Dhan Yojana (PMJDY) scheme as a first step towards digital financial inclusion. The scheme envisions to bring about comprehensive financial inclusion and provide banking services in the form of saving bank account, credit, insurance and pension to each household in the country. Currently, PMJDY has been instrumental in opening of 47 crore bank accounts.²

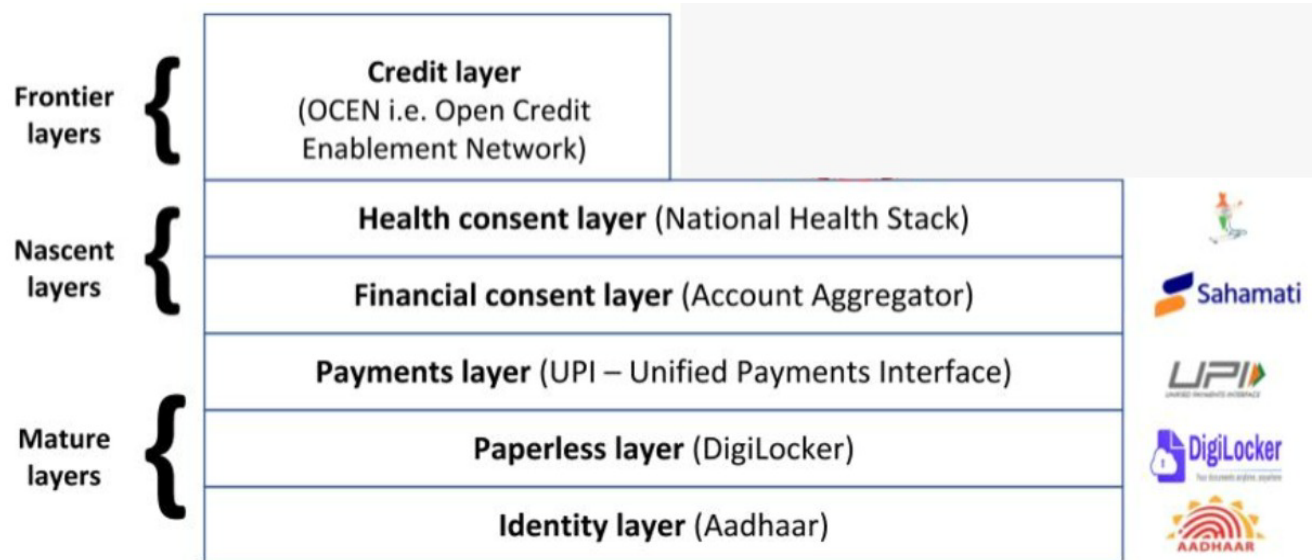


IndiaStack consists of key components such as Universal Payment Interface (UPI), eSign, DigiLocker, eKYC and Data Empowerment and Protection Architecture (DEPA) framework which has been widely adopted by FinTechs in its business processes. DigiLocker has been instrumental in doing away with physical documentation process and allows an individual to download and upload

² <https://pmjdy.gov.in/account/progress-report> (last accessed on 11 January 2022)

FINANCIAL INCLUSION THROUGH ACCESS TO CREDIT

institutional documents in a presence-less and paperless platform. The documents in DigiLocker are issued by an issuing authority using eSign Aadhaar based framework. UPI has been a key driver in revolutionising digital payments by allowing money transfer between any two bank accounts by using a smartphone. eKYC platform is used by FinTech to verify and authentication an individual for customer onboarding purposes. DEPA which is launched in the form of account aggregator allows for managing consent of individuals through an interface for collection and sharing of data.



As per RBI, “financial inclusion is the process of ensuring access to financial services as well as timely and adequate credit where needed by vulnerable groups such as weaker sections and low-income groups at an affordable cost. It also refers to universal access to a wide range of financial services at a reasonable cost. These include not only banking products but also other financial services such as insurance and equity products”.³ In its National Strategy for Financial Inclusion for India 2019-24, the

³ Rangarajan Committee, “Report of the Committee on Financial Inclusion.” (2008) The Government of India. Available at <https://rbi.org.in/scripts/PublicationsView.aspx?id=10494>

FINANCIAL INCLUSION THROUGH ACCESS TO CREDIT

RBI has specified universal access to financial services, providing a basic bouquet of financial services, access to livelihood and skill development, financial literacy and education, customer protection and grievance redressal, and effective co-ordination between various stakeholders, industry players and the government as the focus areas in addressing financial inclusion for India.⁴

National Strategy for Financial Inclusion

Financial inclusion is increasingly being recognised world over as a key driver of economic growth and poverty alleviation. Access to formal finance can boost job creation, reduce vulnerability to economic shocks and increase investments in human capital. At a macro level, greater financial inclusion can support sustainable and inclusive socio-economic growth for all.

To achieve the above objectives in a co-ordinated and time-bound manner, formulation of a National Strategy for Financial Inclusion (NSFI) is essential. Globally, the adoption of the National Financial Inclusion Strategy (NFIS) has been accelerated significantly in the past decade. As of mid-2018, more than 35 countries, including Brazil, China, Indonesia, Peru and Nigeria have launched an NFIS and another 25 countries are in the process of formulating a strategy. Further, several countries have also updated their original NFIS (World Bank, 2018).

The National Strategy for Financial Inclusion for India 2019-24 has been prepared by the Reserve Bank under the aegis of the Financial Inclusion Advisory Committee (FIAC) and is based on the inputs and suggestions from the Government of India, other financial sector regulators viz., Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI) and Pension Fund Regulatory and Development Authority

(PFRDA). This document also reflects various outcomes from wide-ranging consultations held with a range of stakeholders and market players, including National Bank for Agriculture and Rural Development (NABARD), National Payments Corporation of India (NPCI), Commercial Banks, Non-Governmental Organisations (NGOs), and Self-Regulatory Organisations (SROs), etc.

The document includes an analysis of the status and constraints in financial inclusion in India, specific financial inclusion goals, action plan to reach the goals and the mechanism to measure progress. The strategy envisages to make formal financial services **available, accessible, and affordable** to all the citizens in a **safe and transparent** manner to support **inclusive and resilient** multi-stakeholder led growth. It proposes forward looking recommendations to help achieve universal access to financial services through a bouquet of basic financial services leveraging on the BC Model, access to livelihood and skills development, financial literacy and education, customer protection and grievance redressal with effective co-ordination. While the various initiatives have helped in extending financial services to the hitherto excluded sections of society, the strategy aims to focus on deepening the reach, usage and sustainability of financial inclusion. The document was approved by the Financial Stability and Development Council Sub-Committee on March 14, 2019.

Source: Reserve Bank of India, "National Strategy for Financial Inclusion 2019-24" (10 January 2020)."

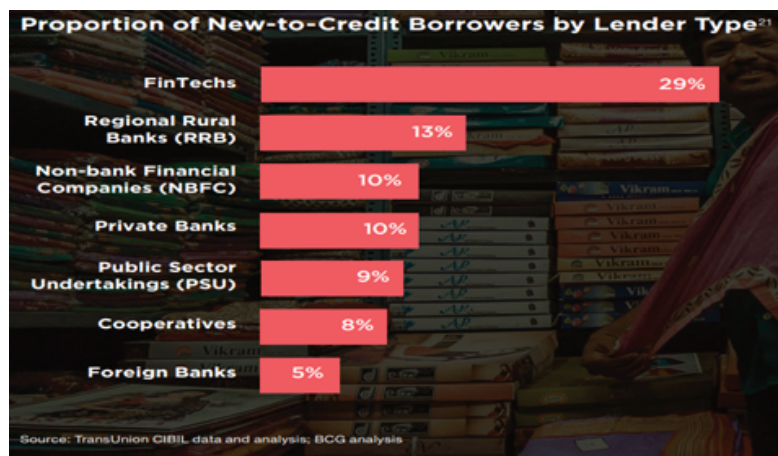
India has also made major strides in creation of a digital infrastructure to deliver services digitally for digital literacy and empowerment of its citizens. "Digital India Programme" launched in 2015 has led to 836 million internet connections in the country as of June 2022.⁵ Additionally, while it is projected that this number will grow to 900 million by 2025, much of this growth will be from the unserved 67% of the rural population.

⁴ Financial Inclusion Plan: A Progress Report, RBI Annual Report, 2019.

⁵ The Indian Telecom Services Performance Indicators, April-June, 2022, Telecom Regulatory Authority of India, 23 November, 2022

FINANCIAL INCLUSION THROUGH ACCESS TO CREDIT

Credit to micro, small and medium enterprises (MSME) industries rose to 19.6% and by 29.7% respectively in November 2022.⁶ Further, MSME credit exposure was INR 23.12 lakh crores as of March 2022, and the year-on-year growth rate was 6.3%.⁷



A key attribute for such exponential growth in digital lending is accessibility of credit through a paperless and presenceless medium where customers have the convenience of accessing credit through their smartphone. Such huge generation of data has led to big data analytics which enables digital lenders to assess a customer's creditworthiness through digital analytics and offer appropriately timed, sized and priced loans to its customers.

⁶ Reserve Bank of India, "Sectoral Deployment of Bank Credit – November 2022", 30 December 2022. Available at https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=54963

⁷ Abhay Kelkar, Vipul Mahajan, Karthik Sundaram, Achin Saharat, "MSME PULSE AUGUST 2022", TransUnion Cibil, SIDBI. Available at <https://www.transunioncibil.com/resources/tucibil/doc/insights/reports/report-msme-august-2022.pdf>

ROLE OF DATA IN INCREASED ACCESS TO CREDIT

As per World Bank's 2020 World Development Report, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies. Countries would gain on average about 4.5% in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5%".⁸

Given the increased use of information and communication technology, primarily through smartphone and affordable internet access, people's daily activities generate a much larger digital footprint which can be utilized for assessing a person's creditworthiness. This increased data phenomenon has also impacted financial institutions and there is a larger shift beyond traditional sources of data for credit scoring and underwriting, as well as use of data technologies along with the conventional statistical techniques.

RBI has described digital lending process as usage of seamless digital technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service.⁹

Digital lending and alternative credit scoring are the fastest growing digital financial services due to their increased demand and collaborative financial inclusion policies by the government. Digital lenders have created alternative credit assessment methods through data to assess individuals in a more inclusive manner for a credit application.

Such alternative data allows a creditor to assess a potential borrower's creditworthiness on various parameters which ultimately results in a more accurate prediction of the borrower's repayment

⁸ World Bank, "World Development Report", (2020). Available at <https://www.worldbank.org/en/publication/wdr2020>.

⁹ Reserve Bank of India, "Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps" (10 November 2021). Available at <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189>.

ROLE OF DATA IN INCREASED ACCESS TO CREDIT

ability. Additionally, the information regarding data used to generate credit reports is very restricted in India and the approach taken by Indian fintechs to address this information asymmetry through utilization of available financial data to provide reliable credit scoring and underwriting promotes inclusivity in the ecosystem. This process also helps new-to-credit borrowers build their credit history which would facilitate their ingress into the formal financial ecosystem and potentially avail more loans, increasing their access to credit.

BENEFITS OF DIGITAL LENDING

A. Seamless loan application process

The turnaround time on credit evaluation, approval and loan disbursement in digital lending is seamless and less time taking in comparison to loan applications assessed through traditional methods. This is especially true for revolving credit facility and small ticket loans mostly availed by neo-prime and sub-prime borrowers.

The reduced turnaround time can be attributed to completely paperless and presenceless application process replacing physical form filings, minimal in-person visits and automated credit assessment through artificial intelligence (AI) and machine learning (ML) algorithms. Digital lenders also utilise cashflow based data as well as other surrogate data from sources such as telecom, utility and social media to evaluate the creditworthiness of a borrower.

B. Reduced operational costs

Traditional lending models have relatively high overhead costs which is attributable to their physical process and feet on street employees involved in the lending process. This leads to increased cost of credit which is ultimately borne by the borrower.

Digital lenders on the other hand have minimal operating costs due to their remote and automated enabled operations and business models which requires minimal human intervention and no physical branch networks. Through this approach, digital lenders are able to maintain nominal fixed costs and facilitate appropriately timed, sized and priced loans to new-to-credit individuals in rural and semi-urban areas as well as MSMEs.

ROLE OF DATA IN INCREASED ACCESS TO CREDIT

C. Reduced feet on street involvement

Digital lenders rely on the borrower's information along with their algorithmic capabilities to structure its repayment and collection process. The collection process generally involves repayment reminders send through a digital medium; b) reaching out to a borrower through calls for any outstanding due to be repaid; and c) an in-house or third party collections team is assigned to the borrower. Repayment methods such as through automatic clearing house (ACH) payment or post-dated cheques, Unified Payments Interface (UPI), digital wallets, etc. have enabled reduction in the turnaround time for the digital lending process.

Other processes such as know your customer process, customer support services and disbursement services are also undertaken digitally by the digital lenders with no or minimal involvement of feet on street employees.

D. Reduced Non-Performing Assets (NPAs)

Digital lenders rely on both traditional and alternatives means for underwriting a borrower's loan application. Such underwriting mechanisms help digital lenders to assess a borrower's creditworthiness through various parameters which ensures minimal delinquencies on the part of the borrowers. The digital lenders deploy their collections and repayments process through digital nudging which helps the borrowers keep track of their loan repayments.

As per RBI's financial stability report, the NPA levels in aggregate consumer credit across all product categories enabled by fintechs stands at just 2% as of September 2022. This is a sharp reduction from the earlier NPA levels of 4.6% in September 2021 for loans disbursed through fintechs.

E. Fraud Prevention

The digital lending application and underwriting process is based on the principle of minimisation of data. The ultimate control over the data rests with the borrower. With the introduction of account aggregators, we can see paradigm shift in data processing standards where the ultimate control on the data only rests with the borrowers.

Digital lenders also invest a lot on their fraud prevention tech stack to ensure that there is no misuse of data. Customer onboarding techniques such as Aadhaar XML based verification and PAN NDSL verification are based on the principle of minimisation which ultimately ensures that only legitimate borrowers get access to credit.

ROLE OF DATA IN INCREASED ACCESS TO CREDIT

As India embarks on its mission of digital financial inclusion, it is critical for the digital lenders to adopt a common mechanism for processing of financial data. The government and regulators should also look at proposing a uniform data processing framework for the digital lending ecosystem and ensure there is harmonisation of laws in this respect.

BROAD GUARDRAILS FOR PROCESSING OF FINANCIAL DATA

DLAI believes that data protection involves securing an individual's privacy as well as allowing them to access a wide variety of financial products. Given the sensitivity and volume of data handled by digital lenders, there is a demonstrable need for a uniform guardrail adopted by the digital lending industry to implement privacy as a design framework for promoting transparency and accountability in data processing mechanism. We have listed out some broad guardrails which can be adopted by the digital lending industry for instituting a privacy by design framework.

1. Data Security

The security and management of data infrastructure includes measures for ensuring availability and integrity of data with the use of regular vulnerability management, malware protection, network boundaries, resource management, distributed denial-of-service, etc. which would complement the data-centric approach to confidentiality. Vulnerabilities in data security can have debilitating effects on digital lenders and their data principals. Infrastructure management should be centred around well-designed and up-to date control processes to avoid errors. Infrastructure security and management is even more important for big data because of the potential domino effect of risks from the increased complexity of data processing.

2. Data confidentiality

The ambit of confidentiality refers to the protection of data in use, transit and rest, and compromises to the same can have a detrimental effect on the data principal and data processor / fiduciary.

The technology and methods for generating and handling data at rest and in transit have evolved over the years, while encrypting data in use is a recent development. The challenges with protecting data in use are compounded for big data because unlike conventional data, big data processing depends heavily on shared computing environments as opposed to local environments, is processed on a continuous basis, and has more longevity on account of being evolving and reincarnating (often through AI/ML solutions).

3. Anonymisation

The sheer volume of personal data increases the chances of indirect identifiability from aggregated data. This can be addressed through privacy-enhancing technologies, either hardware-based (confidential computing), cryptography-based (homomorphic encryption) or data-based (pseudonymisation), which can enable personal data processing with adequate confidentiality safeguards even data use.

BROAD GUARDRAILS FOR PROCESSING OF FINANCIAL DATA

4. Identification, authentication, authorization, and accountability

Identification, authentication, authorization, and accountability (IAAA) is about giving the right person (identification-authentication) the right level of access (authorization) in a timely manner and able to prove due care in that (accountability).¹⁰ Misconfigurations in IAAA can result in major breaches and cause immense loss.

It is impractical to depend primarily on manual provisioning for access management in the world of big data, and fintechs should opt for big data analytics with a focus on identity and access management solutions and a suitable log management solutions. Increasingly, global fintechs are relying on AI/ML solutions which are referred to as identity analytics.

5. Data Portability

Data portability is the right to access, copy your data, and share it with other data controllers and consumers programmatically in order to gain utility from it - is important to enable greater access to services in our digital economy. Financial services, and many others are largely driven by digital platforms that create data about a user based on his or her interactions with the platform, and likely consume information about the user to better provide services. Thus, users should have the ability to share information with service providers for availing a financial product.

6. Uniform Consent Framework

The Data Empowerment and Protection Architecture (DEPA) issued by NITI Aayog discusses about the ORGANS consent framework which highlights the facets of informed consent and preserve individual agency over data sharing. ORGANS is an acronym signifying the following parameters:

- (a) Open Standards – the consent standard is published and designed to operate as an open standard ensuring that all institutions have the same approach to consent and use it in an interoperable manner.
- (b) Revocable – the consent is designed to be revocable at any point in time by the data subject who provided it.
- (c) Granular – consent needs to be provided each time data is shared data as it specifies what data has been requested, how long it will be retained and who will process it.

¹⁰ A Security Analyst, "What is IAAA?" (15 March 2020). Available at <https://securityanalyst.blog/2020/03/15/what-is-iaaa/>

BROAD GUARDRAILS FOR PROCESSING OF FINANCIAL DATA

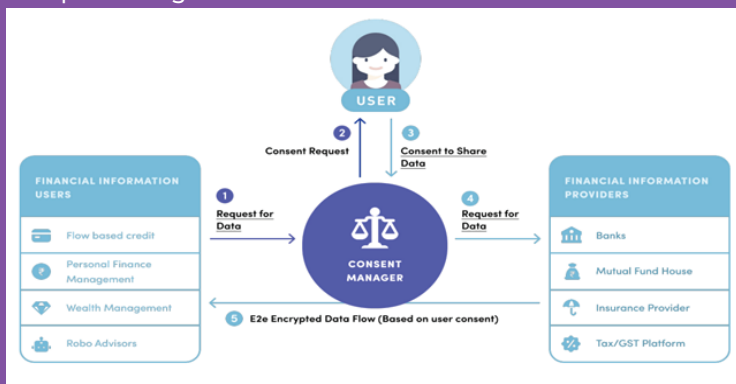
- (d) Auditable – records of all consent provided by a data subject can be retained in machine readable logs.
- (e) Notice – the consent will provide data subjects with notice of the purpose to which it will be put, the parties who will process it and the duration for which it will be retained.
- (f) Secure – the digital consent artefact is secure by design.

This framework provides an excellent starting point for standardising the collection of informed consent at an industry level for the fintech sector. This framework is also largely in line with the requirements for informed consent under the proposed DPDP Bill as well as RBI's Guidelines on Digital Lending (Digital Lending Guidelines) dated 2 September 2022.

The introduction of deemed consent under the DPDP Bill is a welcome move to address the requirement of providing a legal basis for processing data where obtaining consent is impracticable or inadvisable due to pressing concerns. However, deemed consent may only apply in certain situations where the data principal is expected to voluntarily provide data (such as for availing credit) for fair and reasonable purpose after taking into consideration certain prescribed factors. The grounds available under deemed consent framework for processing can be an effective remedy for consent fatigue but for other use cases a uniform consent framework should be deployed to facilitate ease in access in collection, storage and processing of data.

7. Consent Manager

The RBI has mandated the formation of consent managers in the form account aggregators. These function as consent managers for financial data and have a number of benefits associated with them, chiefly more control to the data principal, faster and cheaper exchange of documents, transparency in data flows and accountability for consent processing.



Source: Discussion paper on Data Empowerment And Protection Architecture, NITI Aayog.

BROAD GUARDRAILS FOR PROCESSING OF FINANCIAL DATA

The DPDP Bill also recognises consent managers who shall be entrusted with the task of registering consent of an individual to ensure free flow of information on such consent. A key feature of the account aggregator framework is the validation from each participant in a data sharing transaction to ensure authenticity in such transactions.

The consent framework in the account aggregator ecosystem is also based on the ORGANS framework mentioned above. The benefits of the account aggregator framework ranges from minimisation of multiple consents to reduced cost of data sharing transactions and minimal data breaches since it is based on the principle of minimisation.

INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES

I. Digital Personal Data Protection Bill (DPDP Bill)

The Ministry of Electronics and Information Technology (MeitY) released the draft of the DPDP Bill on 18 November 2022, on which public comments were welcome until 17 December 2022. This is the fourth attempt of the government to introduce India's first standalone data privacy law. This proposed version of the law has undergone several changes from its previous iterations, i.e., the Personal Data Protection Bill, 2018, the Personal Data Protection Bill, 2019 and the Joint Parliamentary Committee's Data Protection Bill, 2021. The DPDP Bill seeks to regulate the processing of digital personal data (personal data collected online or collected offline but digitised).

24 August 2017

Supreme Court, in the case of *K.S. Puttaswamy v. Union of India*, recognised privacy as fundamental right

31 July 2017

Justice B N Srikrishna Committee constituted (Srikrishna Committee) to suggest a draft data protection bill

27 November 2017

Srikrishna Committee released White Paper on Data Protection Framework for India

27 July 2018

Srikrishna Committee submitted Draft Personal Data Protection Bill 2018 (2018 Bill) to MeitY

17 December 2019

2019 Bill was referred to a Joint Parliamentary Committee (JPC)

11 December 2019

Personal Data Protection Bill 2019 (2019 Bill) was tabled in Lok Sabha

10 September 2018

Last date of submissions for feedback on 2018 Bill extended to 10 October 2018

14 August 2018

MeitY invited comments from stakeholders on 2018 Bill by 10 September 2018

4 February 2020

JPC invited comments on 2019 Bill

16 December 2021

JPC tabled its report along with suggested revisions to the 2019 Bill in the Parliament

3 August 2022

2019 Bill (with recommendations suggested by JPC) withdrawn from Parliament

18 November 2022

Draft of Digital Personal Data Protection Bill 2022 released

INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES

A. Applicability

As mentioned above, the DPDP Bill seeks to regulate digital personal data and it does not create further categorisations such as sensitive personal data and critical personal data, as done in the previous iterations.

B. Consent and deemed consent

The DPDP Bill specifies that consent should be free, specific, informed, unambiguous, and through a clear affirmative action. Further, data principals would have the right to withdraw their consent. The DPDP Bill introduces the concept of “deemed consent”, which refers to situations where consent is not explicitly needed, viz. situations where the Data Principal voluntarily provides their data, public interest, among others.

C. Cross-border data transfers

The DPDP Bill does not provide for data localisation requirements. Rather, it stipulates that the government may notify the countries or territories where personal data may be transferred after assessing certain factors that they deem necessary, in accordance with such terms and conditions as may be specified.

D. Rule-making powers of the government

The DPDP Bill has provided immense discretionary rule-making powers to the central government, such that they may frame rules on various issues such as form and manner of reporting data breaches, fair and reasonable purposes for processing personal data without consent, among others.

INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES

II. Digital Lending Guidelines

The RBI set up a working group on digital lending on 13 January 2021 in the backdrop of consumer protection and business conduct concerns within the growing digital lending landscape in India. The working group on digital lending has penned down their recommendations within a report which was released on 18 November 2021. In furtherance of the aforesaid recommendations, the RBI released the Digital Lending Guidelines on 2 September 2022. The key features of the Digital Lending Guidelines are as follows:

A. Collection and usage of borrower data

Collection of borrower data by Digital Lending Apps (DLAs) of Regulated Entities (REs) and Lending Service Providers (LSPs) must be need-based and with prior and explicit consent of the borrower (which must be auditable). The RBI has also clarified that DLAs must refrain from accessing mobile phone resources of borrowers (such as contact list, call logs, and other file and media logs). It has however, permitted DLAs a one-time access for camera, microphone, location, or any other data for the purpose of on-boarding and KYC requirements. Borrowers also have the right to revoke any consent already provided by them for data sharing. Any sharing of data with third parties must be disclosed in the privacy policy of the DLAs and LSPs. The privacy policy should clearly set out the purpose for which borrowers' consent has been requested at each stage of its interface with its borrowers.

B. Storage of customer data

LSPs and DLAs are refrained from storing personal information of the borrowers except some basic minimal data (such as name, address, contact details of the borrower, etc.) required to carry out its operations. The DLAs and LSPs should set out guidelines regarding storage of borrower data including the type of data that can be stored, the length of time for which data can be stored, restrictions on the use of data, data destruction protocol, standards for handling security breach, etc., on its platform.

C. Technology Standards

The RE and its LSPs are required to comply with various technology standards/ requirements on cybersecurity stipulated by RBI and other agencies, or as may be specified from time to time, for undertaking digital lending.

INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES

D. Interplay between the DPDP Bill and the Digital Lending Guidelines

The table below comparatively analyses the provisions of the DPDP Bill and the Digital Lending Guidelines:

	Particulars	DPDP Bill	Digital Lending Guidelines
1.	Subjects	Data fiduciaries and data processors are regulated directly under the DPDP Bill.	REs involved in digital lending are regulated directly under the Digital Lending Guidelines, while their LSPs / DLAs are regulated indirectly.
2.	Cross-border transfer of data	Cross-border transfer of data is permitted to those jurisdictions which are yet to be notified by the central government.	Cross-border transfer of data is barred since all digital lending data is to be stored only in servers located within India.
3.	Deemed consent	Consent is deemed in certain instances for processing data for credit scoring, debt recovery, KYC – fraud checks, among others, under the DPDP Bill.	Prior and explicit consent of the borrowers with clear audit trail is required to be obtained under the Digital Lending Guidelines. Further, RE, LSP and DLAs are prohibited from accessing mobile phone resources, except a one-time access for camera, microphone, and location services for KYC/onboarding requirements. There is no concept of deemed consent under the Digital Lending Guidelines.
4.	Itemised notice	An itemised notice is to be given to the data principal, which must include a list and description of each personal data sought with purpose.	The purpose of obtaining borrower's consent at each stage of interface with the borrowers is to be disclosed as per the Digital Lending Guidelines. REs are required to ensure that

INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES

			<p>their DLAs and LSPs engaged by them have a comprehensive privacy policy compliant with applicable laws, associated regulations and RBI guidelines. For access and collection of personal information of borrowers, DLAs of REs/LSPs should make the comprehensive privacy policy available publicly</p>
5.	Retention of data	<p>The DPDP Bill requires the data to be deleted or anonymised as soon as the purpose of collection of the data is over, or when retention is no longer necessary for legal or business purposes.</p> <p>The DPDP Bill provides that a RE can store KYC related data of an individual as per RBI KYC Master Directions.</p>	<p>The borrower may give consent for data retention, or to make the DLAI delete / forget data. However, under the Digital Lending Guidelines, there is no automatic obligation on the entity to delete the data after its purpose is over.</p>
6.	Third-party Data sharing	<p>Under the DPDP Bill, personal data can be shared with third-parties only pursuant to a valid contract and with prior notice to data principals.</p>	<p>Under the Digital Lending Guidelines, explicit consent of the borrower is needed for sharing of data, except in cases where it is pursuant to a statutory or regulatory requirement. Further, the privacy policy of the DLA must disclose the details of third-parties allowed to collect personal information through the DLA. However, the Digital Lending Guidelines do not mention the requirement of a valid contract.</p>

INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES

7.	Grievance	<p>A grievance redressal mechanism is to be put in place by all data fiduciaries. Significant data fiduciaries have to appoint a data protection officer under the DPDP Bill.</p> <p>Further, it is mandated that the response is to be provided within 7 days post registration of the grievance. If unsatisfied or if the data principal does not get a response within the timeline, they can file a complaint with the Data Protection Board.</p>	<p>Under the Digital Lending Guidelines, the suitable nodal grievance redressal officer is to be appointed by the REs and their LSPs. Responsibility of grievance redressal would remain with the RE.</p> <p>Further, under the Digital Lending Guidelines, the time period for resolution of a grievance is 30 days. If not resolved within the timeline, one file a complaint over the CMS portal under RB-IOS.</p>
8.	Withdrawal / Revocation of consent	<p>Consent for processing of data can be withdrawn by data principals at any time as per the DPDP Bill. Further, it requires the ease of withdrawal of data to be comparable to ease of giving the consent.</p>	<p>Under the Digital Lending Guidelines, the borrower can revoke consent for collection of data. Further, the Digital Lending Guidelines not mention about processing of already collected data, except for the separate option to seek the application to delete / forget the data, and it also does not prescribe the ease of revocation of consent.</p>
9.	Data breach and reporting	<p>Under the DPDP Bill, data fiduciaries and data processors have to adopt reasonable security safeguards to protect personal data in its possession and to prevent breach.</p> <p>In the event of a breach, it has to be notified to the Data Protection Board and to each affected data principal.</p>	<p>Under the Digital Lending Guidelines, REs have to ensure that clear policy guidelines are put in place and disclosed by the DLAs regarding handling security breach.</p> <p>Further, there is no requirement to notify the borrower in case of a data breach. However, CERT-In requirements will still apply in case of data breach.</p>

INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION BILL AND THE DIGITAL LENDING GUIDELINES

10.

Consent Managers

Under the DPDP Bill, data principals may give, manage, review or withdraw their consent to the data fiduciary through a consent manager.

The Digital Lending Guidelines do not provide for a consent manager mechanism.

DLAI'S OBSERVATIONS ON THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

I. Definition of “data fiduciary”

There may be instances when data processors can determine the “means” of processing the data in their own capacity. In a digital lending construct, a LSP, a DLA or a third-party service provider can determine the means of processing of data based on the purposes provided by a lender. For instance, this could be in the form of whitelisting customers as per its proprietary algorithms for enabling credit to an individual. Similarly, there are many back-end technology service providers who determine the means of processing lending data based on the purposes provided to them by a lender.

Hence, including determination of means as a parameter for defining data fiduciaries widens its scope leading to interpretation issues. It also leads to issues in determining on whose instructions the data of an individual is being processed. DLAI recommends that the definition of data fiduciaries should be confined to a person, who alone or in conjunction with other persons, determines only the purpose of processing of personal data.

II. Consistency with other laws

Clause 29 of the DPDP Bill on consistency with other laws states that the DPDP Bill shall be construed in addition to the provisions of other laws. However, it also states that in case of any conflict, the provisions of the DPDP Bill would prevail over the other law to the extent of such conflict. The DLAI seeks clarity as to whether the DPDP Bill would prevail over sector-specific laws or special laws as well, that has prescribed different standards surrounding data basis the nature of data being processed in the industry; e.g., the RBI's Digital Lending Guidelines.

III. Retention of personal data

Clause 9(6) of the DPDP Bill on retention of personal data does not provide the manner of treatment for dormant or inactive user accounts. In the context of digital lending, there are many instances where a customer installs and registers on a digital lending app and deletes it subsequently.

The DLAI recommends that the DPDP Bill may also allow the data fiduciary to take actions prescribed under the said clause on its dormant or inactive user's account.

The DLAI also recommends that the said clause should also allow for deletion of personal data of a data principal after certain duration of inactivity / dormancy even when the user has not specifically requested closure of their account.

Further, the DLAI recommends that the data fiduciary should not be held liable for such deletion of data.

DLAI'S OBSERVATIONS ON THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

IV. Right to information about personal data

The DLAI seeks clarification on clause 12 on right to information about personal data. The DPDP Bill must clarify on whether the data fiduciary is also required to disclose any information of a data principal which was collected by it from a legitimate third-party source.

In the digital lending context, a borrower's data is accessed from third-party sources such as credit information companies and other legitimate sources to assess a borrower's credit worthiness and for verification of their details. Such information is not provided by the data principal (borrower) and cannot be accessed by them as well. The DLAI recommends that the obligation under this clause should be limited to only such information which is collected directly by the lender from the borrower.

V. Right of grievance redressal

In case the intent of the clause is to ensure resolution of a grievance within seven days of a request, the DLAI recommends a longer time period to be prescribed for resolution of a grievance. The DLAI recommends that the clause should be drafted in harmony with RBI's Digital Lending Guidelines which provides thirty days for resolution of a grievance.

VI. Exemptions

Financial services entities are required to comply with various rules, regulations and directions as part of their licensing requirements prescribed by the sectoral regulators.

The DLAI recommends that the exemptions provided under clause 18 of the DPDP Bill should also be extended to processing and / or storage of data in compliance with the licensing requirement issued by sectoral regulators.

VII. Financial penalties

Clause 25 of the DPDP Bill on financial penalties determines the penalties on the discretion of the Data Protection Board and also does not specify any quantifying criteria to arrive at the imposed penalty for any non-compliance.

The DLAI recommends a ceiling-based penalty system that is correlated to the turnover of the data fiduciary. Further, while determining the amount of a financial penalty, in tune with clause 25 (2) (d) of the DPDP Bill, the DLAI recommends that the clause may also add a maximum ceiling of penalty based on a suitable multiple of 'realized gain' or 'avoided loss' which has accrued due to non-compliance.

DLAI'S OBSERVATIONS ON THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

VIII. Deemed consent

The DLAI appreciates the efforts of the Ministry in introducing the concept of deemed consent which can help in avoiding consent fatigue and multiplicity of consents in a data transaction.

The current clause allows for deemed consent for prevention and detection of fraud and for credit scoring purposes. However, the DLAI seeks clarification on how deemed consent can be applicable in the context of credit scoring and prevention and detection of fraud.

IX. Consent notice in multiple languages

The DPDP Bill places an obligation on data fiduciaries to publish consent notices and consent requests in English and in twenty-two languages provided under the Indian Constitution. The platforms offered by digital lenders is majorly available in English or few regional languages. The present obligation will be operationally cumbersome for the digital lending industry to comply with.

The DPDP Bill can take reference from the positions presently adopted by the sectoral regulators in such issues. For instance, the RBI has proposed that all loan related details should be communicated in a vernacular language, or a language understood by the borrower.

RBI allows for a confirmation by a borrower to ensure that the borrower has understood the terms and conditions of the loan.

Similarly, the DLAI recommends that the DPDP Bill should allow data fiduciaries to publish its consent notices / requests in English and in any one other language specified in the Indian Constitution at the option of its customers.

X. Amendments

DLAI recommends that the DPDP Bill must also repeal Section 72A of the Information Technology Act, 2000, and consolidate all the prohibitions and penalties under the DPDP Bill.

CONCLUSION

The key factor for the growth of digital lending in India is enabling paperless and presenceless access to credit to individuals residing in any part of the country. In section 4 of the whitepaper, we have discussed on how digital lending has played a pivotal in reducing the cost of lending in India as well as ensuring reduced NPAs and frauds with its seamless and secure technology framework. Digital lenders have a legitimate interest in an individual's data collected by it in order to enable access to credit to such individuals. Such information is necessary to the functions and activities of digital lenders to protect the interests of all parties in a lending transaction.

With increasing data richness in the country, it is important for the government to provide an inclusive, uniform and harmonious data protection framework which provides for data security and taking into account the anticipated innovations in digital lending in India. The applicability of multiple data privacy legislations for financial sector in India has led to ambiguities in enforcing a uniform data protection standard for financial sector in India. We recommend a single data protection framework for governing financial data in India.

A reflexive based data protection framework will be a key enabler in the growth of digital lending and financial inclusion in India. Harmonisation between different data related legislations in India will be a step forward in democratising credit for underserved and unbanked population of India. DLAI is fully committed towards providing the best-in-class data processing framework for its borrowers to ensure trust, accountability and transparency in digital lending ecosystem. We are also committed towards processing borrower's data only for the specific purposes of providing an appropriately timed, sized and priced loans to each of its borrowers. In order to ensure a sustainable and robust digital lending framework, DLAI and its members will continue to invest in more secure and sustainable technology frameworks.

CONTACT US

SIDDHARTH MAHANOT

Chair- Knowledge committee
smahanot@indifi.com

PRIYASHMITA GUHA

Director
priyashmita@dlai.in

dlai

www.dlai.in

DIGITAL LENDERS ASSOCIATION OF INDIA