Data security & data privacy in the era of digital lending:

Laws in India and other jurisdictions

Ajay Kumar K V
Vinod Kothari & Company

Kolkata:
1006-1009, Krishna Building
224 AJC Bose Road
Kolkata – 700 017
Phone: 033 2281 3742
Email: corplaw@vinodkothari.com

New Delhi:
A-467, First Floor,
Defence Colony,
New Delhi-110024
Phone: 011 41315340
Email: delhi@vinodkothari.com

Mumbai:
403-406, Shreyas Chambers
175, D N Road, Fort
Mumbai
Phone: 022 2261 4021/ 6237 0959
Email: mumbai@vinodkothari.com

Index

- Meaning of Digital Lending
- Digital Lending: Indian scenario
- Understanding jargons
- Digital Lending Models
- Data Security
- Global principles of data privacy
- Regulatory Framework India & Abroad

Digital Lending Process

1. Customer application

Customer requests for a retail loan- capture of digital data

2. KYC

verify a customer's identity and address digitally via Aadhaar authentication

3. Credit bureau check

Automated check of customer credit behaviour

4. Automated sanction

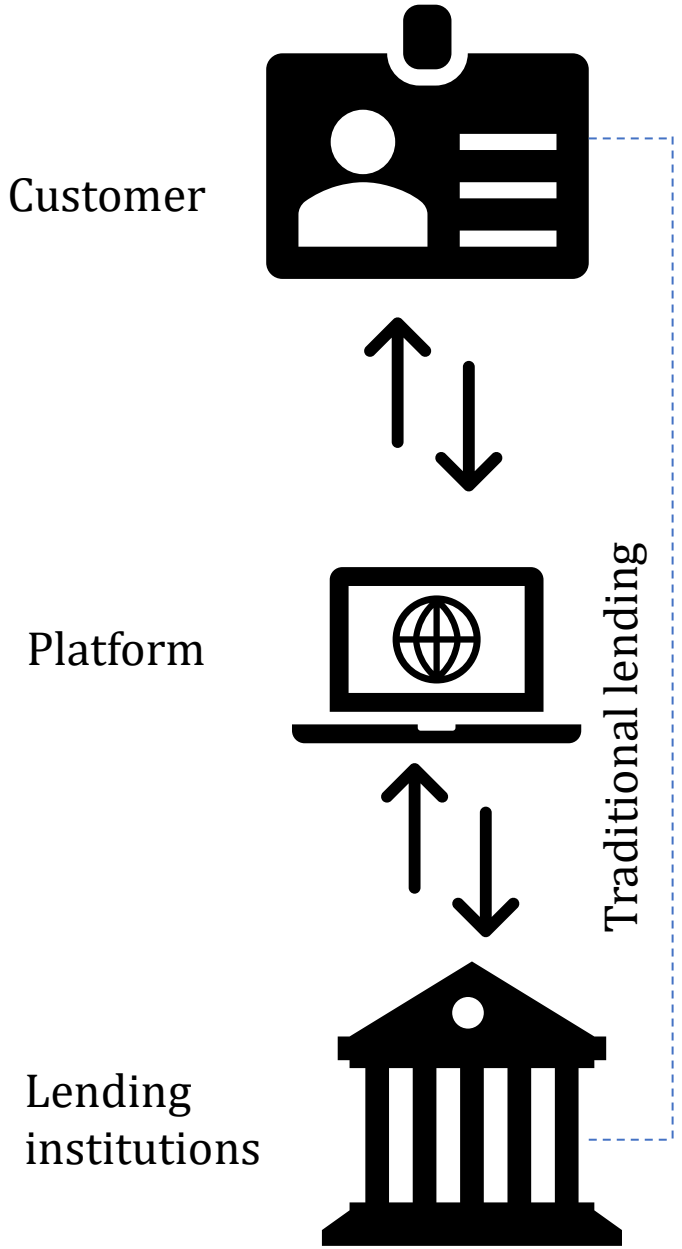
Automated rules check using questions an external data

5. Digital disbursement & execution

Once approved, the customer digitally signs and stamping is done online

6. EMI & servicing

The fund is disbursed instantly to the customer's account and a SI is created for EMI payment



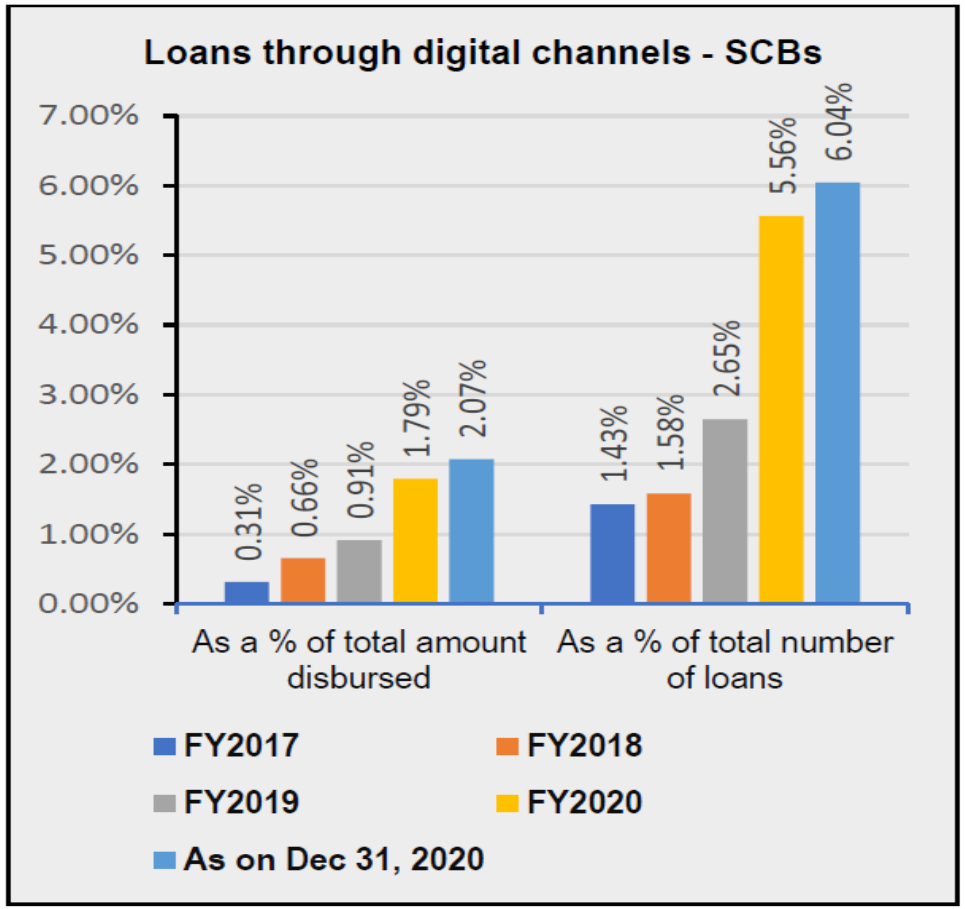
Meaning of Digital Lending ('DL')

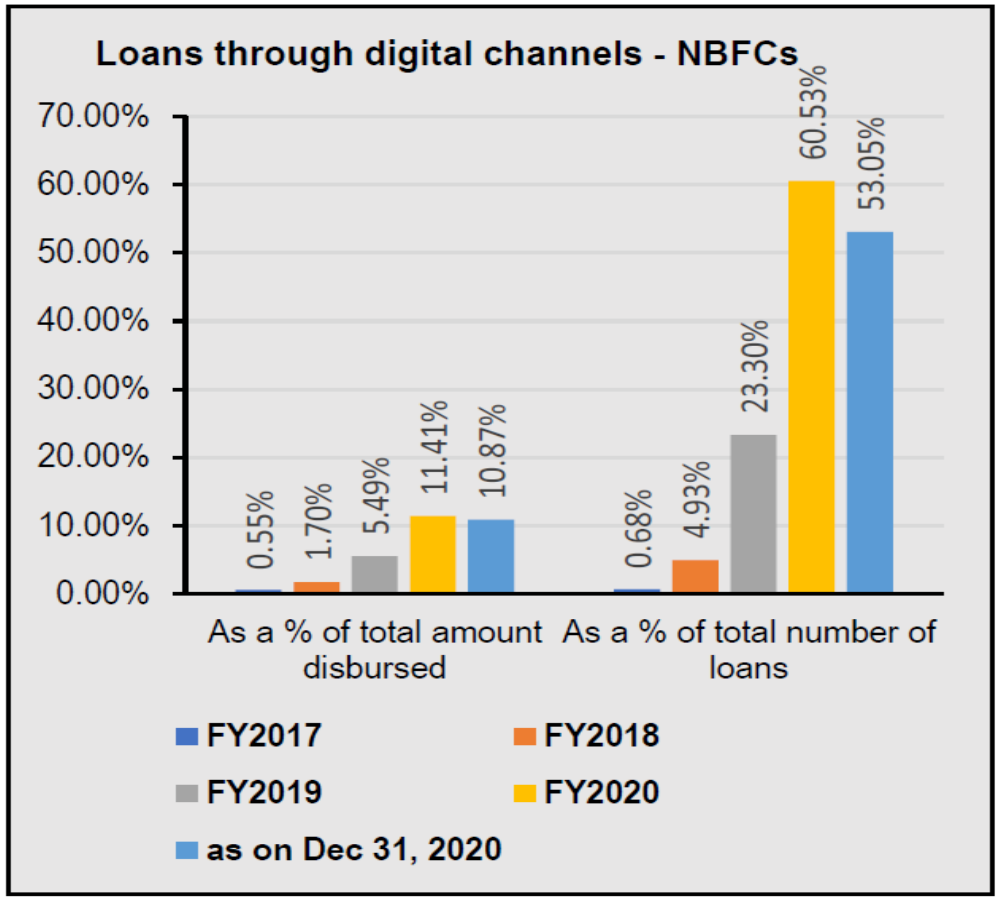
- DL is a subset of Fintech
- Financial Stability Board (FSB) defines fintech as-

  "FinTech is technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services".

- A remote and automated lending process, majorly by use of seamless digital technologies in customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service.

Digital Lending: Indian scenario



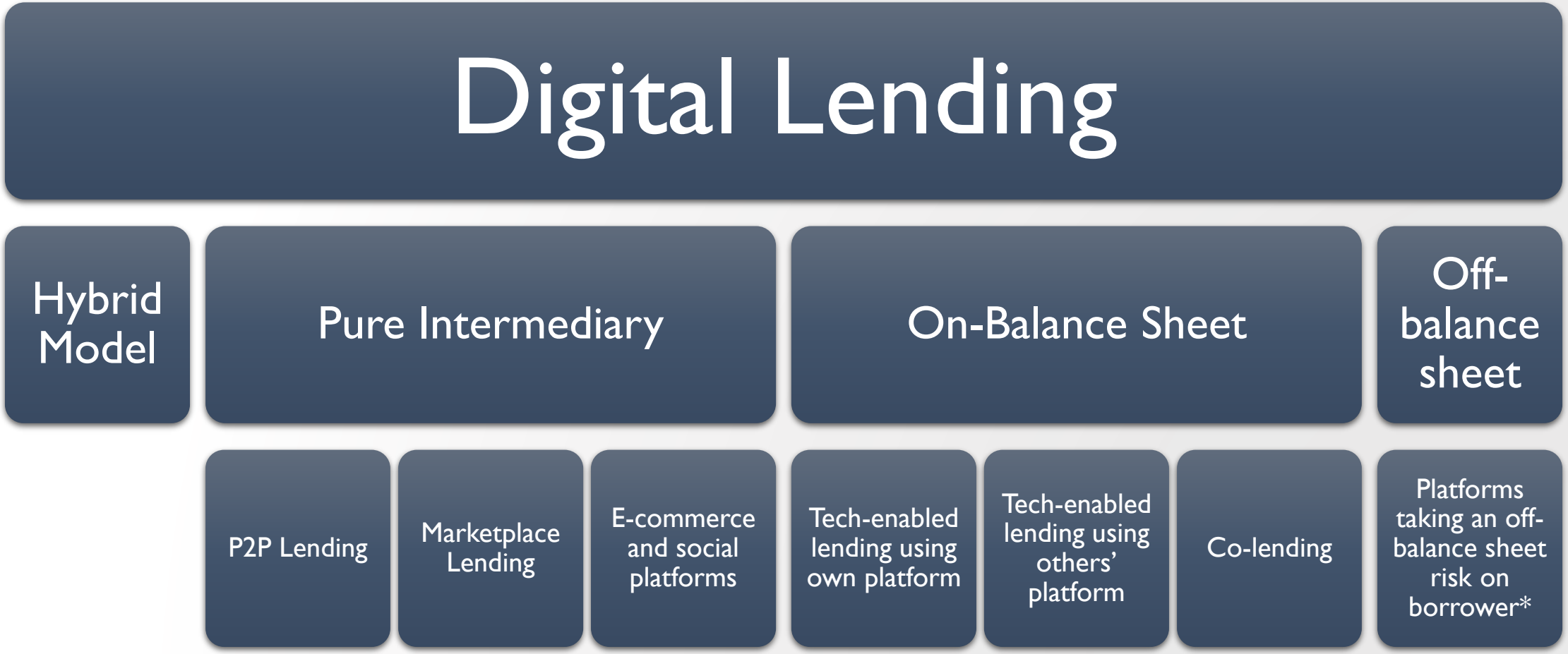


Source: RBI-WG Report on DL

Understanding jargons

- **Platform**: Online interface such as app/website that enable interaction of lender and borrower and facilitate the process of lending transaction
- **Outsourcing**: In the context of digital lending, the process of getting some of the elements of the lending process- such as sourcing customers, processing information etc. done from a service provider.
  - A platform in a digital lending transactions (unless owned by the lender) is a service provider under an outsourcing arrangement
- **Lending Service Providers** : Agents of a balance sheet lender (banks, NBFCs etc.) who carry out one or more of the lender's functions such as customer acquisition, underwriting support, pricing support, disbursement, servicing, monitoring, collection, liquidation of specific loan or loan portfolio for compensation from the balance sheet lenders.
- **Marketplace lending or P2P lending**: A mode of lending wherein several customers meet several lenders over a platform and undertake lending transactions.
- **Regulated Entities (REs)**: Entities that are regulated by the RBI- banks, NBFCs, HFCs, AIFIs, SFBs, UCBs etc.
- **Balance Sheet Lending**: Financial service involving extension of monetary loans, where the lender retains the loan and associated credit risk of the loan on its own balance sheet.
- **Cyber Security**: Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction.

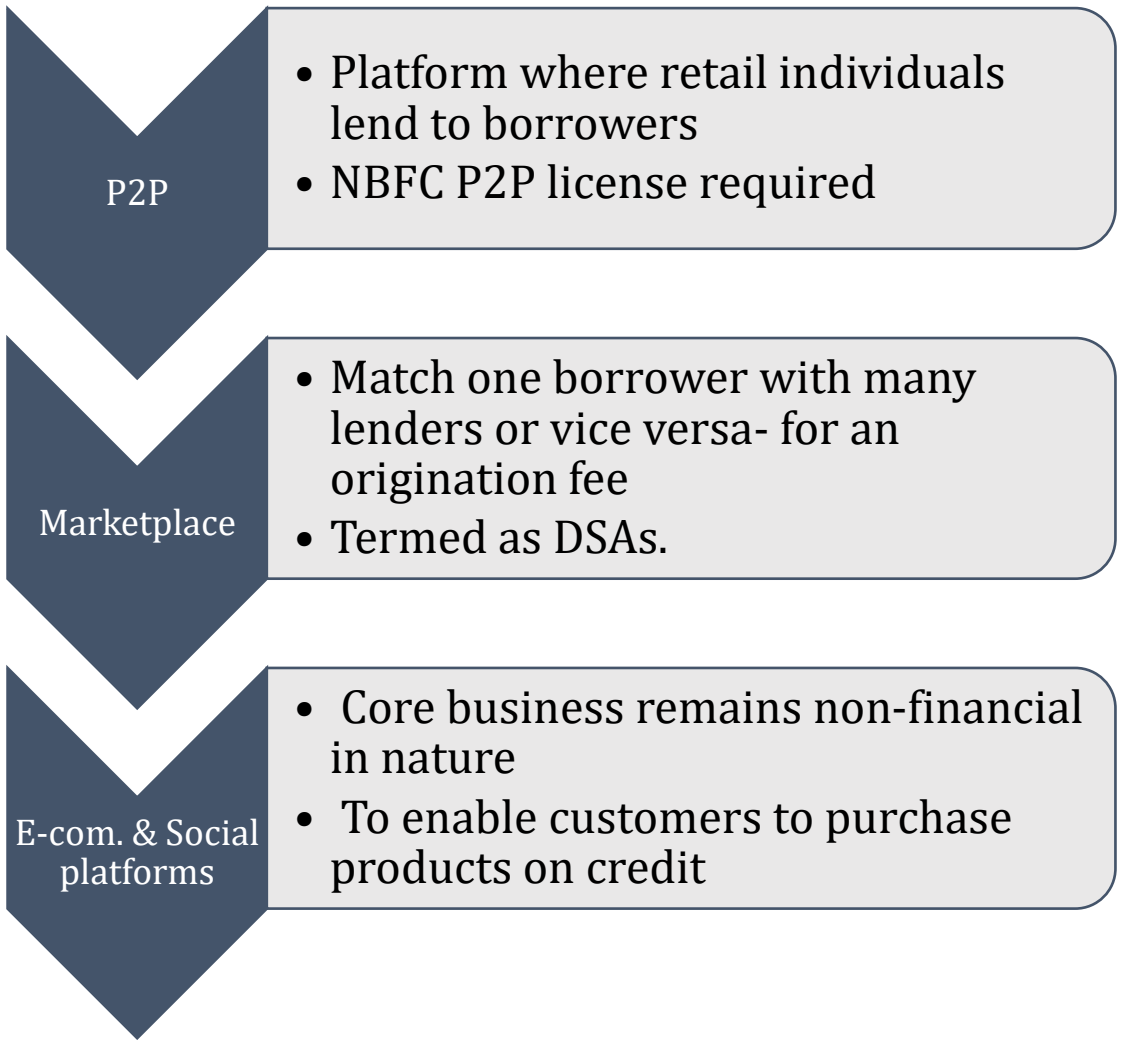
Digital Lending Models



Loans end up on the balance sheet of another lender

Pure Intermediary Models

- Platform serves as an online-lending intermediary or as a sourcing partner for financial entities/lenders
- Loans are originated in the books of financial entity or lenders
- Platform receives its commission or fees for every customer sourced by it
- Prudential Norms for P2P:
  - Minimum NOF- Rs. 2 crores
  - Leverage restriction- Maximum 2
  - Restriction on own balance sheet lending including credit enhancement support,
  - Limits on exposure of lenders on customer and overall lending limits applicable
  - Secured lending not allowed
- Platform responsible for customer on-boarding, loan documentation, disbursement and recovery of funds (escrow mechanism), KYC, Credit Evaluation, CIC Reporting



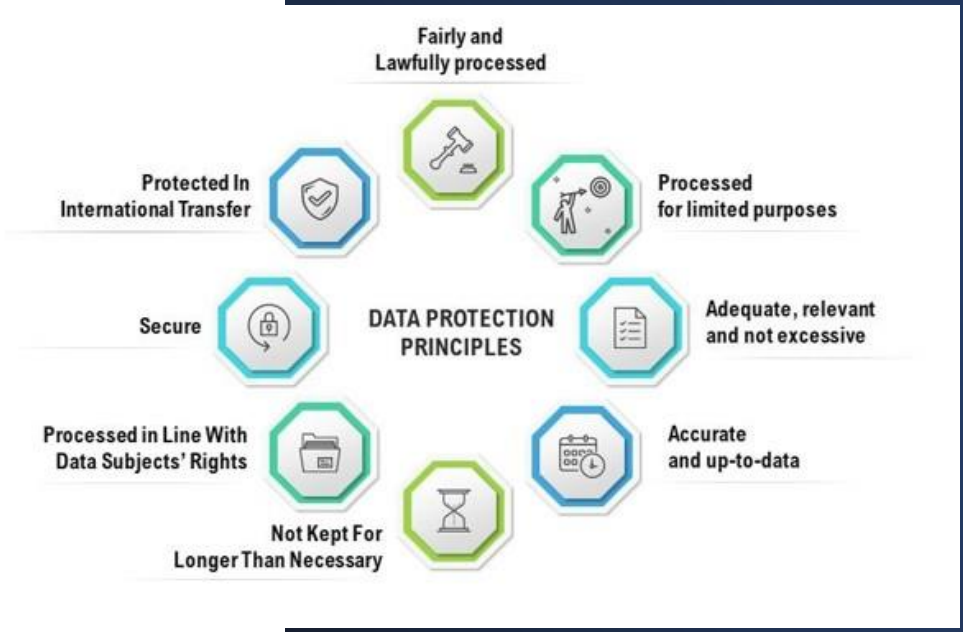
Data Security

What & Why data security?

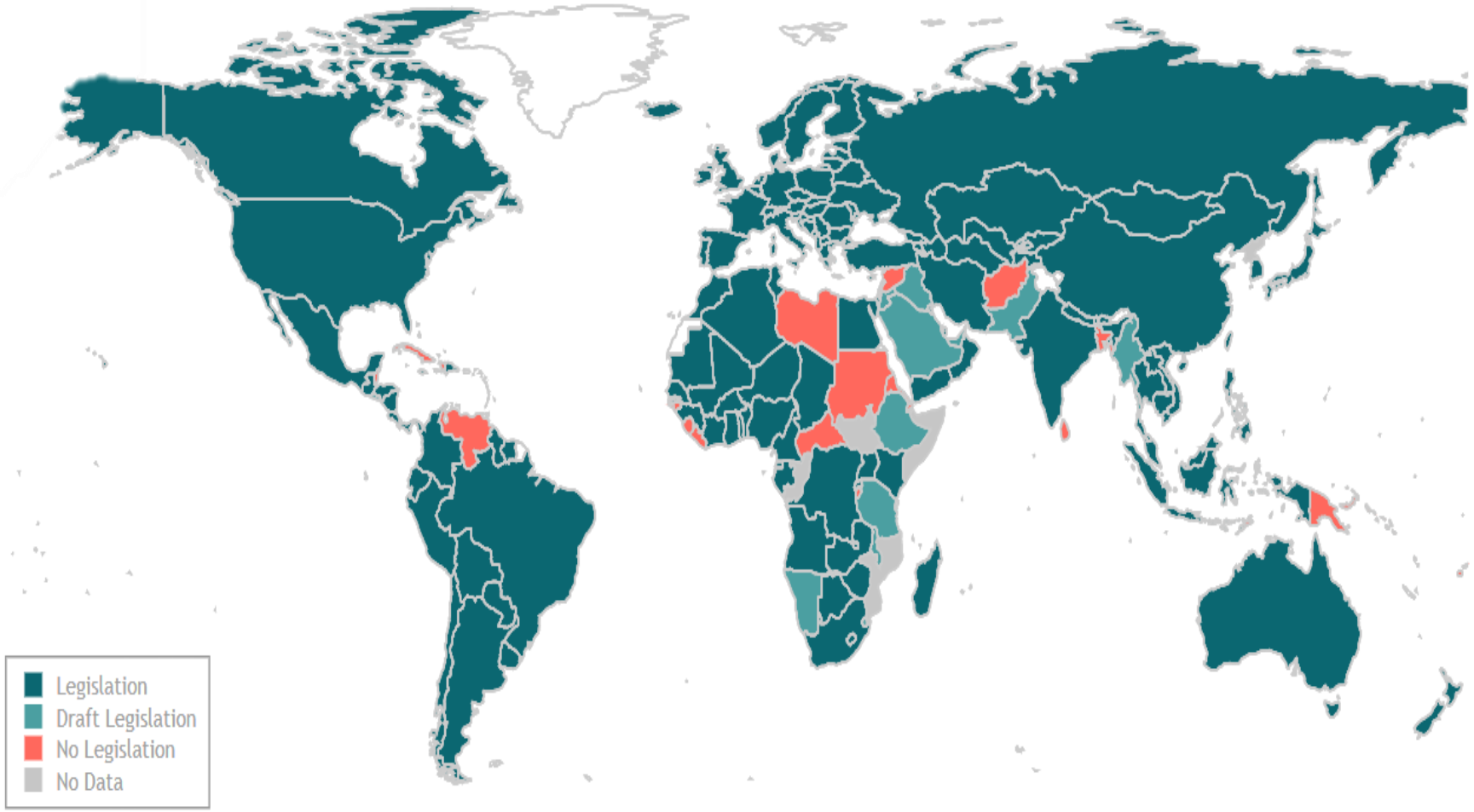
- Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.
- To prevent from fraudulent activities, hacking, phishing, and identity theft, etc.
- To prevent unauthorized sale of data to third party businesses.
- At macro level: India's economic, national security and data protection concerns.
- Data protection in DL:
  - Involves personal data, including financial/credit information;
  - Accesses mobile devices of users including contacts, messages, photo gallery, etc.
- Exchange of information happens at various stages right from application till disbursal
- Compliance with privacy laws to be ensured for effective growth of DL

Global principles of data privacy

- Notice – advising users, visitors, readers to protect personal information.
- Choice and consent – providing people with choices and consent around the use, storage, management and collection of personal information.
- Access and participation – ensuring the information is accessed and used by the correct people within the right security protocols.
- Integrity and security – ensuring that the data is secure and that there is no unauthorised access.
- Enforcement – ensuring that the service, site, solution and platform are aligned with some form of regulation that enforces compliance.



Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

Regulatory Framework

- The Information Technology Act, 2000
- The Credit Information Companies (Regulation) Act, 2005
- Know Your Customer Directions
- Outsourcing Guidelines and Fair Practice Code

India (1/5)

❑Information Technology Act, 2000

- Defines sensitive personal data or information (passwords, financial information such as Bank account or credit card or debit card or other payment instrument details, etc.)

- Section 43A - primarily deals with compensation (no upper limit) for negligence in implementing and maintaining reasonable security practices and procedures in relation to sensitive personal data or information (“SPDI”).

- Section 72-A - punishment for disclosure of information in breach of lawful contract or without the information provider’s consent (imprisonment for a term extending to three years and fine extending to Rs. 5 lakh)

India (2/5)

❑Credit Information Companies (Regulation) Act, 2005

- CICRA provides the privacy principles which shall guide the CICs, Credit Institutions and Specified Users in their operations in relation to collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information.

- Credit Institutions : Banking Company, NABARD, RRBs, NBFCs, HFI, PFI, SFCs, etc.

- Specified User : Credit institutions, Credit information company, Persons/institutions as may be specified (Insurance company, TRAI registered cellular/phone service companies, Stock broker, trading member, SEBI, IRDAI)

- Section 17(4) prohibits “disclosure” of “credit information” received by a CIC:
  - By CIC to any person other than its Specified User
  - By Specified User, to any other person
  - By CIC or Specified User for any other purpose than as permitted or required by law

Sharing of Credit Information

Authorisation

Sourcing Arrangement

Unauthorized User No Sourcing Arrangement	Authorized User No Sourcing Arrangement
Unauthorized User With Sourcing Arrangement	Authorized User With Sourcing Arrangement

India (3/5)

❑Know Your Customer Directions

- Para 55 of the KYC Directions provides for secrecy obligations
- To maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
- Information collected from customers for the purpose of opening of account shall be treated as **confidential** and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
- The exceptions to the said rule shall be as under:
  - where disclosure is under compulsion of law
  - where there is a duty to the public to disclose,
  - the interest of bank requires disclosure and
  - where the disclosure is made with the express or implied consent of the customer.

❑Data Localisation Requirements for Cards

- The RBI had on April 6, 2018, issued a circular requiring all payment system participants and banks to store payments data in India only
- Action against MasterCard due to non-compliance

India (4/5)

❑Outsourcing Arrangements

- In case of outsourcing, confidentiality requirements applicable on the financial institution shall apply on the service provider as well:
  - shall have a specific condition for data confidentiality;
  - must state that confidentiality must be maintained even after agreement expires;
  - access of information to employees of service provider shall be on need to know basis
  - must be capable of isolating details of financial institutions' customers at all times
  - the financial institution and the RBI to have the right to access books or conduct inspection of the service provider at any time
  - to report to the RBI in case of any breach of confidentiality by service provider
  - the NBFC would be liable to its customers for any damages

❑Adherence to Fair Practices Code

- Chapter VI of NBFC Master Directions applicable to NBFCs with customer interface
- RBI Circular dated June 24, 2020 directed all Banks and NBFCs to ensure adherence to FPC and outsourcing guidelines irrespective of whether they lend through their own digital lending platform or through an outsourced lending platform.
- Concerns of exorbitant interest rates, non-transparent methods to calculate interest, harsh recovery measures, unauthorised use of personal data and bad behavior.
- Ensure to disclosure of name of platforms on the website, disclosure to the customer about name of the lender, to issue sanction letter in the lender's letterhead before disbursal, issue of loan agreement along with all enclosures, effective oversight & creation of awareness about the grievance redressal mechanism

India (5/5)

❑ Personal Data (Protection) Bill, 2019*

- **Applicability**: The "Bill" will apply only to data collected, stored and processed in digital form.
- **Definition:**
  - **SPD**: personal data, which may, reveal, be related to, or constitute— (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15.
  - **financial data**: means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history
- **Data localization**: The Bill proposes that sensitive personal data must be stored in India only.

Major highlights:

- **Punishment**: The offences punishable under the scope of the Bill shall be cognizable and non-bailable. The criminal penalties include imprisonment of up to three years and a fine of two lakh rupees.
- **Section 11** - the consent must be free, specific, clear, capable of being withdrawn and most importantly – it must be informed as per Section 7 of the Bill.
- **Section 7** - every data fiduciary shall give to the data principal, a notice at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable.
- **Section 12 –** provides for exceptions to section 11 (sharing of data without consent)
- **Privacy by Design Policy-** Data fiduciaries must prepare a privacy by design policy as per Section 22
- **Data Protection Officer**- every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations

*Withdrawn by CG on 3rd Aug. 2022

USA

- No single principal data protection legislation; the country follows a sectoral approach to data privacy, relying on a patchwork of sector-specific laws and state laws
- The California Consumer Privacy Act (CCPA) gives residents of California four rights that give them more power over their personal data: right to notice, right to access, right to opt in (or out) and right to equal services. Any organization that collects the personal data of California residents, not just businesses located in the state, must comply with CCPA
- The Gramm-Leach-Bliley Act 1999, governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial services industry.
- The US senate will soon be considering the draft American Data Privacy and Protection Act (ADPPA), a federal privacy bill that would regulate how organizations keep and use consumer data of US citizens.

UK

- The U.K. is currently regulated by the Data Protection Act 2018 which incorporates the EU GDPR and supplements its provisions.
- The Data Protection Act 2018 focuses significantly on data subject rights, “special category” personal data, data protection fees, data protection offenses, consent from children and enforcement.
- Information Commissioner's Office (ICO) is the independent body responsible for enforcing the Data Protection Act.
- UK data protection laws don’t allow organisations to transfer personal data outside the UK, except in circumstances that include:
  - where the recipient is located in an EEA country
  - where the recipient is located in a non-EEA country but the data protection regime in that country is considered "adequate" for the purposes of UK data protection laws; or
  - where appropriate safeguards for the protection of personal data are in place.

South Africa

- Data privacy issues are regulated under the Protection of Personal Information (PoPI) Act 2013, several sector-specific laws and the common law.
- Based on 8 principles that broadly discusses:
  - Rules for collecting, using and processing data
  - Ensuring the quality of the information
  - Upholding standards of transparency and openness
  - Efforts to safeguard against loss, damage or destruction of data
- The Constitution of the Republic of South Africa 1996 regulates more general privacy provisions. Section 14, in particular, upholds the general right that all citizens have to privacy.
- Information Regulator supervises the provisions of the Act and promotion of the same .

China

- China's most recent privacy law took effect in May 2018.The Information Technology – Personal Information Security Specification (GB/T 35273-2017), apparently contains more strenuous requirements than the GDPR.
- Security audit on personal data controllers:

  a) It shall audit the privacy policy and related procedures, as well as the effectiveness of security measures;

  b) It shall establish an automated audit system, to monitor and record personal information processing activities;

- Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) (PI Specification) Amendment 2020
  - voluntary in nature, setting out best practices concerning protection of personal information (PI);
  - place more weight on the independence of will of individuals in deciding whether to share one's PI as a condition of access to products and services that offer Business Functions (most mobile apps);
  - third-Party connection management in data sharing;
  - establishment of PI protection personnel and department
  - establish & maintain PI processing record.

EU-GDPR

- The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world.
- Applicability: European Union (EU), and it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.
- Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified.
- GDPR's Article 30 lays out that most organisations need to keep records of their data processing, how data is shared and also stored.
- Organisations that have "regular and systematic monitoring" of individuals at a large scale or process a lot of sensitive personal data have to employ a data protection officer (‘DPO’).
- 7 protection and accountability principles outlined in Article 5.1-2:
  - Lawfulness, fairness and transparency - Processing must be lawful, fair, and transparent to the data subject.
  - Purpose limitation - You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
  - Data minimization - You should collect and process only as much data as absolutely necessary for the purposes specified.
  - Accuracy - You must keep personal data accurate and up to date.
  - Storage limitation - You may only store personally identifying data for as long as necessary for the specified purpose.
  - Integrity and confidentiality - Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
  - Accountability - The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Regulatory framework: Snapshot

Particulars	India	USA	UK	SA	China	EU
Specific Legislation	✗*	✓	✓	✓	✓	✓
DPO	✓	✗	✓	✓	✓	✓
Data Localisation	✓	✗	✗	✗	✗	✓
Audit	✓	✗	✓	✗	✓	✗
Specific Regulator	✓	✗	✓	✓	✓	✓
Penal provision	✓	✓	✓	✓	✓	✓

*Note that PDP Bill 2019 was withdrawn on 03.08.2022

Thank You