



Cambridge
Centre
for Alternative
Finance



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Digital Insurance India

www.bfaglobal.com | [@bfaglobal](https://twitter.com/bfaglobal)

UPDATED 31 MARCH 2021

Funded by





Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School



Disclaimer

To the best of our knowledge, the information contained herein is accurate and reliable as of the date of publication.

However, **BFA Global** and the **Cambridge Centre for Alternative Finance** do not assume any liability whatsoever for the accuracy and completeness of the deck, and we provide no warranty, expressed or implied, in respect thereof. The provision of the information contained in this deck does not constitute legal or financial advice nor opinions of any kind. No advisory, fiduciary, or other relationship is created between us and any person accessing or otherwise using any of the information provided herein. **BFA Global**, the **Cambridge Centre for Alternative Finance**, any of their directors, officers, employees, agents, or contributors will not be liable for any damages, losses, or causes of action of any nature arising from any use of any of the said information.

Relevant Regulations

1. Insurance
2. Data protection
3. Consumer protection
4. AML / KYC
5. Competition
6. Taxation

The Cambridge Centre for Alternative Finance (CCAF) and BFA Global have produced this deck to support fintech startups working in India and those seeking to enter the Indian fintech market in navigating the regulatory environment.

This deck provides **an overview of India's regulation of digital insurance**.

Each slide in this deck provides high-level facts about each of the relevant regulations as well as a link to the original source. Not all regulations included in the deck may be relevant based on the nuances of your particular business model.



01 — Insurance



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Insurance: Overview

—

Key regulation: The Insurance Act, 1938 (as amended) and the **Insurance Regulatory and Development Authority of India Act, 1999** (as amended)

—

Main regulator: Insurance Regulatory and Development Authority of India (IRDAI)

—

Overview of regulation of e-insurance and Insurtech activities:

- Guidelines on Repositories and Electronic Issuance of Policies Guidelines, 2015 detail the establishment and regulate the functioning of **Insurance Repositories (IR)**. These are companies licensed by IRDAI that maintain records of insurance policies in electronic form on behalf of insurers. It mandates every insurer issuing and maintaining 'e-insurance policies' utilize the services of an IR and enter into service level agreements with one or more IRs
- IRDAI Issuance of e-Insurance Policies Regulations, 2016 creates different thresholds for annual premiums and sums insured for different lines of **e-insurance businesses**.
- IRDAI Guidelines on Insurance e-commerce, 2017 enables insurers and insurance intermediaries to set-up **Insurance Self-Network Platforms** to sell and service insurance policies.
- IRDAI Insurance Web Aggregators Regulations, 2017 regulates **web aggregators** that maintain insurance price comparison and insurance information comparison websites as an insurance intermediary.

Insurance: Licensing requirements

Key regulation: The Insurance Regulatory and Development Authority (Registration of Indian Insurance Companies) Regulations, 2000 prescribes the licensing requirements for Indian insurance companies.

Licensing process:

- An applicant wishing to apply for a license is required first to make a requisition for registration application. This requisition must be accompanied by other documents, including a memorandum of association, articles of association, details of directors and principal officer, and a statement indicating class of insurance business and sources of shared capital (see Sec. 5(2)).
- Upon acceptance of the requisition, the applicant can apply for the license. The application must be accompanied by an application fee of INR 50,000 (US\$690.13) per class of insurance business (see Sec. 15) and other documents such as proof of minimum capital, prospectus, etc. (see Sec. 10).
- Applicants must demonstrate at least INR100 crore (US\$13,500,000) of paid up equity share capital, if the application for grant of certificate is for life insurance business or general insurance business. The capital entry requirement for regular insurers and micro insurers under the present regulation are the same, but there is a proposal under consideration to reduce these requirements for micro insurers (see slide 66 for details).
- The IRDAI, while granting authorization, considers factors such as past record of promoters, capital structure, nature of insurance products, etc. (see Sec 12).

Insurance: Foreign reinsurers & sandbox

- The licensing and authorization of branches of foreign reinsurers is governed by IRDAI (Registration and Operations of Branch Offices of Foreign Reinsurers other than Llyod's) Regulations, 2015 (as amended). The regulations prescribe the procedure of requisition (Section 3 to 10), licensing authorization (Section 11 to 17), and other operational issues (Section 28).
- The IRDA also issued the IRDAI (Regulatory Sandbox) Regulations on July 26, 2019 with the objective of striking a balance between the orderly development of the insurance sector and the protection of interests of policyholders while also facilitating innovation.



Insurance: Microinsurance

Key regulation:

IRDAI (Microinsurance)

Regulations 2015 governs micro-insurance policies, which promote insurance coverage among economically vulnerable sections of society. Insurance policies for Micro, Small and Medium Enterprises (MSME) are considered microinsurance policies.

Licensing process:

- No separate licensing is required for an insurance business to enter the microinsurance business.
- A life insurer business can offer a life microinsurance product but is required to have a tie-up with a general insurer business to provide general microinsurance products, Meanwhile, a general insurer business can offer a general microinsurance product but is required to have a tie-up with a life insurer business to provide life microinsurance products (Sec 3).
- For the purpose of distribution and solicitation, all intermediaries registered with the IRDAI are also empowered to distribute microinsurance products without needing a separate registration.

Entry level capital:

- The license application for microinsurance requires evidence of INR1 Billion (US\$1381 million) or more in paid up equity share capital. This applies to both life insurance businesses and general insurance businesses.
- The IRDAI committee has proposed a reduction in entry-level capital requirements for standalone micro-insurance companies to INR200 million (US\$28 million) from the current requirement of INR1 billion (US\$1381 million). The goal of the proposed change is to accelerate the expansion of this segment of the insurance market in India.

02 — Data protection



Data protection: National provisions

Key Laws:

Information Technology Act, 2000 ("IT Act") and its corresponding Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("IT Rules"), and the Indian Constitution

Main provisions:

India does not currently have national legislation governing data protection or privacy. Therefore, regulation is fragmented:

- Personal data is recognized as a fundamental right under Article 21 of the **Indian Constitution**, as ruled by the Supreme Court of India.
- The **IT Act** provides legal recognition of transactions carried out via electronic data interchange and other means of electronic communication.
- Section 43A of the IT Act confers liability on companies which possesses, deals, or handles any sensitive personal data in a computer for any wrongful loss or gain to any person caused due to negligence in implementing and maintaining reasonable data security practices and procedures
- Section 72A of the IT Act states that if any person secures access to personal information while providing contractual services and discloses the data without the consent of the concerned person(s) to any other person shall be punished with a fine and/or imprisonment.
- IT Rules provides individuals with the right to access and correct their information on online platforms. It also mandates that any company collecting sensitive personal information publishes an online privacy policy to which users must agree. Companies must obtain consent of the individual before disclosing sensitive personal information except in the case of law enforcement.
- A comprehensive data protection law - the Personal Data Protection Bill 2019 is currently pending before Parliament

Data protection: Sectoral provisions

The primary legal instruments that address data protection in the financial sector include:

Credit:

- The Credit Information Companies (Regulation) Act, 2005 (CIC Act) and the Credit Information Companies Regulation, 2006 (CIC Regulations) recognize credit information companies (CICs) as collectors of information and requires they adhere to privacy principles at the collection stage and uphold those principles during use and disclosure of credit information. CICs are further required to ensure the credit information they hold is accurate, complete, and protected against loss or unauthorized use, access, and disclosure.

KYC data:

- KYC norms limit the categories of information that banks and financial institutions can seek from their customers. Once such information is collected, there is an obligation on banks to keep it confidential. Any such information collected must not be divulged by the regulated entities under the RBI's purview for the purpose of cross-selling or for any other purpose without the explicit permission of the customer.
- There are similar regulations such as the Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs, the Master Circular on Customer Services, 2009, and the Code of Banks Commitment to Customers etc. These create restrictions on the cross-selling of information and impose customer confidentiality obligations

Sources: [The Credit Information Companies \(Regulation\) Act, 2005](#), [the Credit Information Companies Regulation, 2006](#), [Master Direction - Know Your Customer \(KYC\) Direction, 2016](#), [Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs](#), [the Master Circular on Customer Services, 2009](#), [the Code of Banks Commitment to Customers](#)

Data protection: Sectoral provisions (cont.)

Insurance:

- In the Insurance sector, Insurance Act, 1938 and regulations issued thereunder by the IRDAI, such as IRDAI (Maintenance of Insurance Records) Regulations, 2015, IRDAI (Health Insurance Regulations), 2016, IRDAI (Protection of Policyholders' Interests) Regulations, 2017, and IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 impose confidentiality provisions.
- Intermediaries in the insurance sector such as corporate agents, third party administrators (TPAs), and web aggregators serve as a bridge between customers and insurance companies by facilitating the process of purchasing insurance products and assisting in the servicing of policies and assessment of claims. These intermediaries also bear confidential information and thus are subject to obligations relating to data protection and preservation of confidentiality, as prescribed by the IRDAI. Each type of intermediary is subject to its own regulations and Code of Conduct. With relation to TPAs, the IRDAI (Third Party Administrators – Health Services) Regulations, 2016 prohibits TPAs from sharing the data and personal information of customers they receive from servicing insurance policies or claims.

A [report](#) by the Ministry of Electronics and Information Technology has mapped the various financial sector laws that contain data protection provisions.

Data protection: Data localization & cybersecurity

Data localization:

As there is no comprehensive framework, data localization requirements can be found in sectoral regulations on data protection:

- Per India's 2013 Companies Act, Indian registered companies must maintain their books of account for audit and inspection only in India.
- The IRDAI mandates that all original policyholder records be maintained in India.
- On April 6, 2018, the RBI issued a circular titled Storage of Payment System Data, which mandated that all payment system providers store their payment systems data on servers located within the territorial jurisdiction of India. However, for the foreign leg of the transaction, it is permitted to store the data in the foreign country, if required.

Cybersecurity:

- The RBI, under the Guidelines on Regulation of Payment Aggregators and Payment Gateways, provides comprehensive baseline technology recommendations for Payment Gateways.
- The SEBI released Master Circulars on creating Cyber Security Resilience Framework for Stockbrokers and for Asset Management Companies.

Data sharing: Open banking

- Under India's Open Banking approach, customers control their data via NBFCs called Account Aggregators (AAs). AAs act as licensed intermediaries that are responsible for the customers' consent management and consolidate customers' financial information held with different financial entities and spread across financial sector regulators. AAs act as an intermediary between Financial Information Provider (FIP), such as banks, non-banking financial companies, insurance companies, insurance repositories, pension funds, etc., and Financial Information User (FIU), which are entities regulated by any financial sector regulator. The flow of information occurs through Application Programming Interfaces (APIs).
- The transfer of information requires explicit customer consent and with appropriate agreements/authorizations between the AAs, the customers, and the FIPs. Data cannot be stored by the AA or used by it for any other purpose. The regulations also set out explicit and robust data security and customer grievance redressal mechanisms. To protect customers' interest, the AAs are not permitted to undertake any other activity.
- Further, to facilitate seamless movement of data and consent-based sharing, a set of core technical specifications were framed in November 2019 by the Reserve Bank Information Technology Private Limited (ReBIT), a wholly owned subsidiary of the RBI, for adoption by all regulated entities acting either as FIPs or FIUs.
- To protect users' critical financial information and enforce a mechanism for obtaining proper consent from customers, AAs must obtain consent through a standardized electronic consent format as prescribed under regulations. AAs must inform the customer of all the necessary attributes contained in the consent format and the customer's rights to file complaints. Customers are able to revoke consent, following which a new consent would have to be obtained. Explicit onus has also been placed on FIPs to verify the validity of the consent, its specified date and usage, and the credentials of the AA.

03 — Consumer protection



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Consumer protection: National provisions

Key Laws: Consumer Protection Act, 2019

Main provisions:

- The Consumer Protection Act provides for speedy redressal of all consumer complaints through designated consumer protection redressal forums at the District, State, and National levels.
- The Act vested wide-ranging powers with these redressal forums, starting from search, seizure, and summons to meet the needs of the changing times.
- The Consumer Protection Act also includes e-commerce platforms and electronic service providers under its purview to apply more accountability to online platforms and service providers.



Consumer protection: Sectoral provisions

Each financial sector regulator has issued its own consumer protection provisions:

RBI:

- The RBI has formulated a "Charter of Customer Rights" for banks based on global best practices around consumer protection. Banks are required to either prepare their own board-approved policy incorporating the five rights of the Charter or suitably integrate their existing customer service policy with the "Model Customer Rights Policy" formulated by Indian Banks' Association (IBA) / Banking Codes and Standards Boards of India (BCSBI).
- The RBI has three ombudsman schemes - one for banks, a second for NBFCs and a third for digital transactions. The RBI has suggested a potential new ombudsman scheme to unify these schemes to make the mechanism simpler, efficient, and more responsive.
- The ombudsman scheme for digital transaction is implemented by the RBI to enable a protection mechanism for digital payments service providers with relation to unauthorized electronic fund transfers (EFTs) and other digital transaction issues. The scheme contains detailed complaint procedures and a dispute resolution mechanism with a strict timeline for resolving issues. The Ombudsman can award monetary damages for any breach of regulations.

IRDAI:

- The IRDAI issued the IRDAI (Protection of Policyholders' Interests) Regulations, 2017 to ensure the interests of insurance policyholders are protected. Per Regulation 17, every insurer must have in place proper procedures and effective mechanisms to resolve complaints and grievances of policyholders and claimants efficiently and speedily.

Consumer protection: Sectoral provisions (cont.)



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

SEBI:

- SEBI set up the Office of Investor Assistance and Education to protect the interests of investors. It issued SEBI (Aid for Legal Proceedings) Guidelines, 2009 to help investors raise complaints and the SEBI (Investor Protection and Education Fund) Regulations, 2009 whose funds are used to protect investors and promote investor education and awareness.
- SEBI also established online investor complaints redressal system called “SCORES” to address investor complaints against listed companies or regulated entities in the securities market.

Unified complaints forum:

- All the financial regulators, along with state and law enforcement authorities, created a single consumer awareness and complaints forum where consumers can lodge complaints against any illegal activity carried out by the offending entities.
- The forum can be accessed [here](#).

04 —

Anti-money laundering (AML)/know your customer (KYC)



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

AML/KYC: Key laws & main provisions

Key Laws:

- Prevention of Money Laundering Act, 2002 (PMLA, as amended)
- PML (Maintenance of Records) Rules, 2005
- Aadhaar Act
- Master Direction - Know Your Customer (KYC) Direction, 2016

Master Direction KYC:

- Applies to all entities regulated by RBI.
- These directions lay out KYC guidelines (Sec. 5), Customer Identification procedures (Sec. 13 and 14), and Customer Due Diligence procedures (Chp. 6) for each type of customer.
- RBI's officially valid KYC documents include passports, permanent account number cards issued by income tax authorities, driving licenses, voter identity cards, and job cards issued under the rural employment guarantee scheme.

Digital KYC:

On February 25, 2016, RBI introduced “Digital KYC” mechanisms in Section 3 of its amended Master Direction on KYC.

- Digital KYC involves capturing a live photo of the customer and an officially valid document or the proof of possession of Aadhaar where offline verification cannot be completed.
- RBI has further introduced Video based Customer Identification Process (V-CIP) which involves a customer-consent requirement to undertake the Customer Identification Process (CIP).
- Digital KYC and V-CIP KYC is permitted for all entities regulated by RBI.

AML/KYC: Key laws & main provisions (cont.)

PML Rules:

- Lay out the procedure and manner of maintaining, and time for furnishing, information and verification of records of the client identity.
- Mandate record maintenance of and allow sectoral regulators to issue their own procedures for maintenance of records.

Aadhaar Act (EKYC):

- Aadhaar Act established the Unique Identification Authority of India (UIDAI), which manages the specific data collected about Indian citizens. The UIDAI permits the instant verification of biometric and demographic details of the holder through e-verification which is routed via the Aadhaar database (i.e., e-KYC).
- However, the Supreme Court's judgement in *Justice Puttaswamy (Retd.) v. Union of India* denied private entities access to the UIDAI server for e-verification of holder information for KYC. It also restricted the use of Aadhaar as a mandatory KYC document for a limited number of services and permitted banks' access to Aadhaar only with the consent of the holder.

- In collaboration with the industry, the UIDAI released new e-KYC systems to ensure smooth continuation of business. These include the use of XML files, masking of data, and use of QR codes. The accounts opened through these e-KYC mechanisms have certain restrictions on usage.

AML/KYC: Securities, outsourcing & confidentiality



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Investment

SEBI issued Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT)/ Obligations of Securities Market Intermediaries. This Master Circular requires all SEBI-registered entities have AML policies in place and lays out the manner and procedure to maintain records.

Outsourcing KYC

Banks, NBFCs, and other Regulated Entities (RE) may engage third parties for data collection for KYC purposes and rely on the third party's customer due diligence. However, REs are required to ensure that decision-making to determine compliance with KYC norms is not outsourced.

Confidentiality

There are Secrecy Obligations and restrictions on sharing KYC information (Section 56 of Master Directions). Information collected from customers for the purpose of opening an account is treated as confidential and related details cannot be divulged for the purpose of cross selling or for any other purpose without the express permission of the customer.

05 — Competition



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Competition: Relevant legislation & regulatory powers



Competition Act:

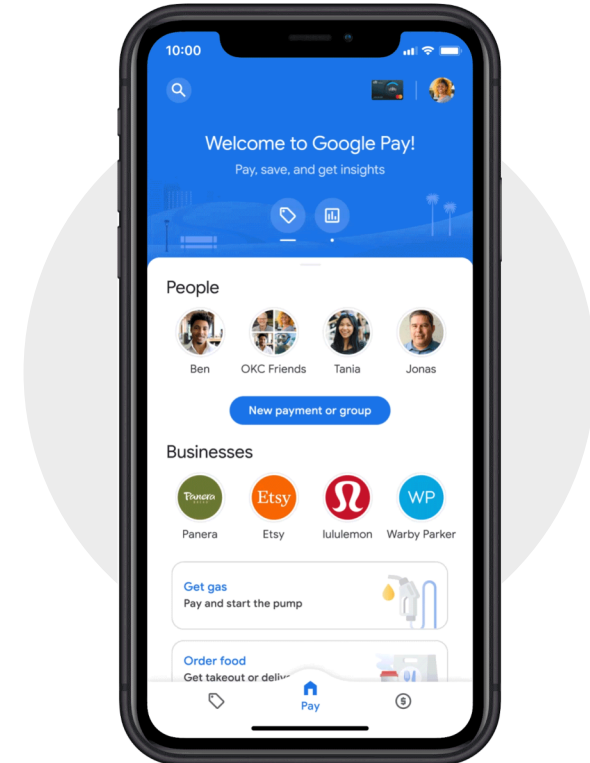
- The Competition Act, 2002 regulates various types of business activities.
- Section 3 of the Act prohibits vertical and horizontal anti-competitive agreements (e.g. between cartels) which causes or is likely to cause an appreciable adverse effect on competition (AAEC).
- Section 4 prohibits market players from abusing their “dominant position” by clearly prohibiting practices like predatory pricing that create a barrier to entry for new players.
- Section 5 regulates combination agreements (i.e. mergers or acquisitions) to prohibit them from hindering fair competition in the market.

Competition Commission of India:

- The Competition Act, 2002 establishes the Competition Commission of India (CCI). The CCI is responsible for eradicating anti-competitive practices, promoting and sustaining competition in markets, protecting consumers’ interests, and ensuring freedom of trade for other participants in markets (Section 18)
- Section 19 of the Act empowers the CCI to initiate an inquiry against a business organization for violation of Section 3 or 4.
- Section 19 also stipulates the factors the CCI will consider in determining if an arrangement or an activity causes an AAEC and if it should be deemed void.
- Section 20 empowers the CCI to initiate an inquiry against combination agreements for violations of Sections 5 and 6 and outlines the factors that must be considered to determine whether an agreement causes an AAEC in the market.

Competition: Focus on fintech

- The NPCI recently released a circular and Standard Operating Procedure mandating all Third-Party Application Providers such as Google Pay and PayPal to not exceed 30% of the overall volume of transactions processed in UPI payments.
- As recently as November 2020, the CCI ordered detailed investigation into Google Pay's activities for possible violations of Section 4 of the Competition Act.



06 —

Taxation of financial services



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Taxation: Financial services

Tax incentives:

- The Start-up India initiative seeks to promote and incentivize startups by providing certain tax waivers for startups incorporated after 1 April 2016.
 - This includes a 100% tax rebate on profits for a total period of 3 years within a period of 10 years.
 - The tax incentive scheme has been extended until the end of the financial year 2022.
- A new section 54 EE was inserted in the Income Tax Act for eligible startups to exempt their tax on long-term capital gains within a period of six months from the date of transfer of the asset if such a long-term capital gain or a part thereof is invested in certain funds designated by Central Government as exemptible. To date the Central Government has not designated any funds as exemptible.
- There are tax rebates for merchants accepting more than 50% of their transactions digitally and for merchants providing cash back incentives to consumers for making payments of their GST Bills via prescribed digital modes.

Normal tax rate:

- If the given financial service does not fall within any exemption or promotion scheme of the Government of India, then it shall be subject to corporate tax regime under the Income Tax Act 1960.

For more information and further guidance on engaging with regulators see [Fintech Regulation in India](#)

www.bfaglobal.com

info@bfaglobal.com

[@bfaglobal](https://twitter.com/bfaglobal)



Cambridge
**Centre
for Alternative
Finance**



UNIVERSITY OF
CAMBRIDGE
Judge Business School