ADVOCATES & SOLICITORS

Data Protection Obligations of Financial Service Providers in India

Office: +91 11 41727676
Mobile: +91 9560439503 | 8586074575
Email: anuroop@akandpartners.in

Table of Contents

Constitutional Right to Privacy

Right to Privacy is a fundamental right under Right to Life[1]. Supreme Court of India has acknowledged that 'Right to Privacy' includes 'Informational Privacy' that deals with a person's mind. The Supreme Court's explanation of 'Informational Privacy' lays down the foundation of India's data protection regime, guaranteeing individuals the means to control the usage and access of their personal data.[2]

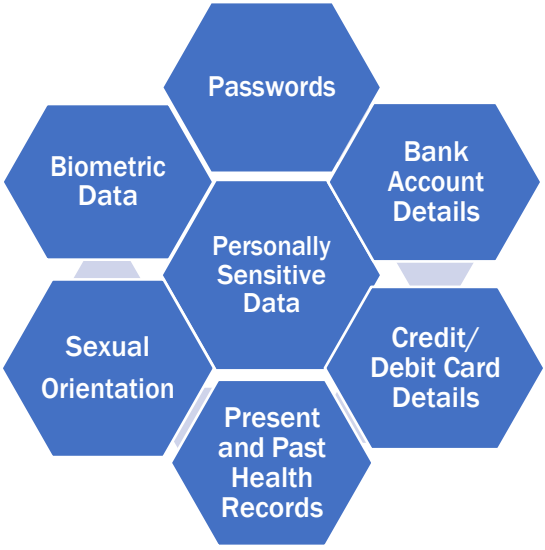
[1] Article 21, The Constitution of India, 1950.
[2] *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1.

Regulation and Enforcement

In the Indian financial sector, data protection regulations have broad provisions that directs handling both personally sensitive information as well as financially sensitive information.

Standards for Personally Sensitive Information

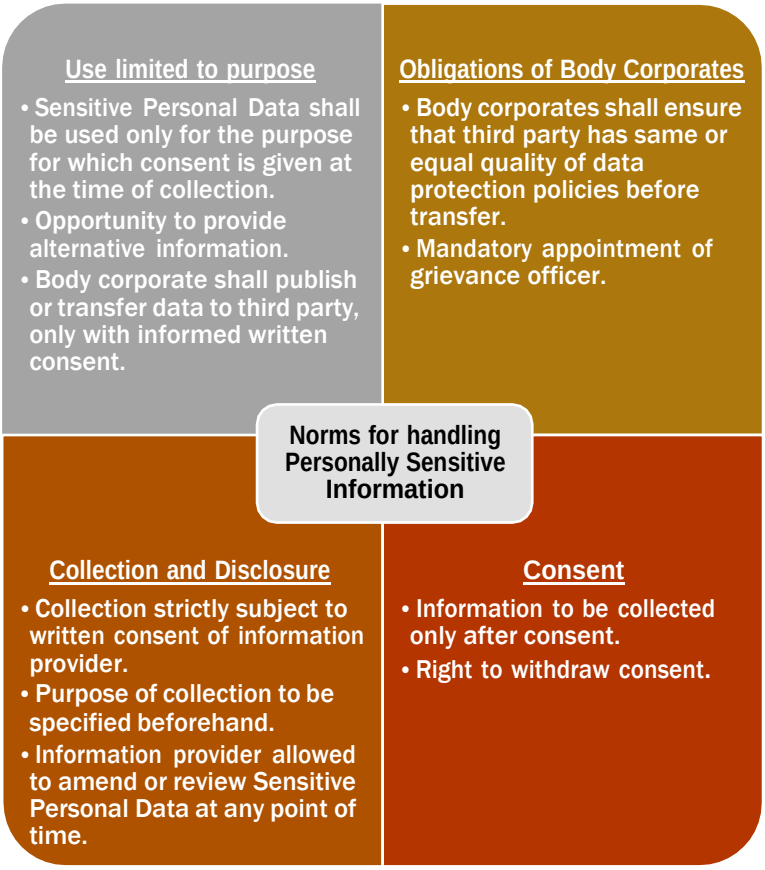
The Information Technology Act, 2000[3] and its rules are the primary framework which governs handling of personally sensitive information in India. There are certain norms that



are mandatory for all body corporates and person located in India handling any personally sensitive information. Any negligence in implementation and maintenance of the same

[3] The Information Technology Act, 2000.

attracts damages by way of compensation to the person so affected.[4]



[4] Section 43 A, The Information Technology Act, 2000.

Standards for Financially Sensitive Information

A financially sensitive information like bank details, credit records, transactional data, etc., is a subset of personally sensitive information. Being specific to finance sector, financially sensitive information is also regulated through industry specific regulations. These regulations cover the obligations of all financial sector service providers.

For regulatory purposes, financial service providers can be broadly classified into: regulated financial entities (i.e., all banks and non- banking financial institutes) and financial technology companies (i.e., companies that are not regulated financial entities but are engaged in financial service's business).

India's central bank and financial regulator, Reserve Bank of India (RBI), governs and ensures the regulations for protection of all types of financially sensitive information. Apart from RBI, other entities also govern the digital financial data.

A snapshot of major regulations governing financially sensitive information is as follows:

RBI's Guidelines on Digital Lending		
Regulated Entities (REs)	**Key Features**	**Key Obligations**
• All commercial banks • All cooperative banks (except rural cooperative banks) • All Non-Banking Financial Companies (NBFCs)	• Allowed to collect financially sensitive information through third party digital lending applications (DLA) • Allowed to transmit financially sensitive information to a lending service partner (LSP) (i.e., any agent hired to carry out one or more lender's functions like recovery, monitoring etc.).	• Thorough initial and period audit to ensure LSPs are compliant with data privacy norms • DLA collect data on need-based with prior explicit consent • DLAs to desist from accessing mobile phone resources such as file, media, call logs, contact, etc. except for onboarding purposes • REs to ensure LSPs do not store personal information except basic minimal data required to carry out operations • DLAs to have a comprehensive functional privacy policy

RBI's Tokenization Scheme

Entities Regulated

- All payment system providers
- All payment system participants

Key Features

- The scheme has extended the device-based tokenization framework to Card-on- File Tokenization

Key Obligations

- The regulation mandates replacement of actual card details with an alternate code called 'token', which shall be unique for a combination of card.
- The regulation states that no entity other than the card issuer and/ or card networks shall store the card/ transaction details.

Computer Emergency Response Team of India (CERT-In) Guidelines

Entities Regulated

- All digital service providers
- Data centers
- Data intermediaries
- Body corporates
- Government organizations

Key Features

- All regulated entities shall create and enable logs of all of their information and communication technology (ICT) systems and maintain them securely for a period of 180 days in India.

Key Obligation

- All logs shall be maintained only in India
- Logs shall be furnished and provided to CERT-In immediately upon its request or upon filing of any cyber complaint of data security breach, which shall be filed within 6 hours of noticing such incidents.

RBI's Master Direction on Digital Payment Security Controls

Entities Regulated

- Banks
- Non- Banking Financial Companies (NBFCs)

Key Features

- Lays guidelines for regulated entities to establish a robust digital payment systems security control for online payments.

Key Obligations

- The entities regulated are obligated to maintain payment application security since its deployment by adhering to existing data protection standards like guidelines in ISO, threat catalogs by NIST etc.
- Entities regulated are obligated to implement multi-factor authentication for wire transfer. These authentications must be implemented based on a risk assessment.
- Entities are required to implement security controls to identify any suspicious transaction behaviour.

The Payment and Settlement Systems Act, 2007

Entities Regulated

- All service providers in payment and settlements related activities, whether located in India or abroad

Key Features

- Gives a minimum standard to manage risks (including data leakage risk) in outsourcing of payment and settlement related activities, including onboarding of customers

Key Obligations

- A system provider i.e., a person who operates an authorized payment system is debarred from disclosing the existence and contents of any documents or information given to him by a system participant to any person

RBI's Cyber Security Frameworks in Banks

Entities Regulated	• All schedules commercial banks, excluding regional rural banks
Key Features	• The framework recognized the sophistication of digital banking and highlights the need to put in place an "adaptive incident response", management and recovery framework to deal with adverse incidents like data leaks.
Key Obligations	• Entities regulated are obligated to establish a Cyber Security Baseline and Resilience. The framework provides some basic indicative list for the same. • Banks are obligated to establish a Cyber Security Operations Centre, which shall be responsible for proactive monitoring of sophisticated tools for detection of incidence of data security breach. • Banks are obligated to notify RBI of any "unusual" cyber- security incidents whether successful or not, instantly within 6 hours.

Indian Data Privacy vis-a-vis GDPR

Particulars	GDPR - UK	Indian Legislations
Personal Sensitive Data	Any information relating to an identified or identifiable natural person	Passwords, Bank Account details, Credit/debit card details, Present and past health records, Sexual orientation & Biometric data
Data Identification	'Pseudonymization' of personal data recommended but not mandatory	RBI tokenization scheme mandates replacement of actual card details with an alternate code called 'token', which shall be unique for a combination of card.
Processing	Prohibits processing special categories of personal data unless conditions are satisfied (e.g., explicit consent, necessity of processing	Mandatory consent before processing, privacy policy to have notice of processing activities, the types of data collected and purposes for collection, any disclosure practices, and descriptions of their security safeguards.
Data Localization	No data localization requirement	RBI regulated entities to store all data on Indian servers
Right to be Forgotten	Available	Option to borrower to revoke consent and if required, delete/ forget data

Our Team

Anuroop Omkar
Founder & Partner

Kritika Krishnamurthy
Founder & Partner

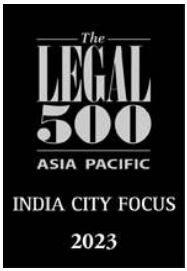
Shreyas Mehrotra
Head of Dispute Resolution

Nidhi Bhatia
Director (Singapore)

Arjun Bikas Dutta
Director (Former General Manager, Reserve Bank of India)

Prasanna Kumar Dash
Director (Former Member, Central Board of Direct Taxes, Government of India)

Awards & Recognitions



Top Law Firm in Banking & Finance

If you like this handbook, do read the

AKP Insights on the recent Personal Digital Data Protection Bill here (*Scan the QR Code now*)

DISCLAIMER

This update is for general information purposes only. This document may contain copyrighted material on a fair use basis. If you wish to use any copyrighted material from this update beyond 'fair use', please obtain permission from copyright owners. Please obtain professional advice before using this information for business purposes.

For more information, contact us at

Office: +91 11 41727676
Mobile: +91 9560439503 | 8586074575
Email- anuroop@akandpartners.in
C 18, Third Floor, LSC 1, C Block Market,
Vasant Vihar, New Delhi
110057