



**DSCI Sectoral Privacy Guide**

# Banking

Research Partner:



## Disclaimer

---

The content of the publication has been collected, analysed and compiled with due care based on the information and sources believed by DSCI to be reliable, available at the date of publication. However, DSCI disclaims all warranties as to the accuracy, completeness, or adequacy of such information. DSCI shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. Readers of this publication are advised to seek their own professional guidance before taking any course of action or decision, for which they are solely responsible. It is highly advised to take note of the current Government and Sectoral regulations in place at the time of any practice implementation as they are subject to change from what has been represented now. The material in this publication is copyrighted but allowed for free distribution. You may not, however, modify, reuse or use the contents of the report for commercial purposes, including the text, graphics, presentations, etc. without DSCI's written consent.

**Copyright ©2023 | All rights reserved.**

---

# CONTENTS

---

<b>1. ABOUT THIS GUIDE .....</b>	<b>04</b>
<b>2. INTRODUCTION .....</b>	<b>06</b>
An Overview of the Banking Sector in India.....	07
Digitisation in India's Banking Sector.....	09
Changes in the Banking Ecosystem Due to Digitisation .....	11
The Role of Digitisation in the Banking Sector .....	13
Policy Developments on Data Privacy in the Banking Sector .....	15
<b>3. KEY CONCEPTS AND FRAMEWORKS.....</b>	<b>16</b>
Banking Sector Participants .....	17
Key Data Privacy Concepts .....	21
Tracing the Journey of the Banking Consumer.....	23
<b>4. THE CHALLENGE OF CONSUMER PRIVACY IN BANKING.....</b>	<b>34</b>
Ensuring Compliance with Existing Regulations on Data Privacy .....	35
Preparing for New Obligations Amidst Rising Data Privacy Risks .....	44
<b>5. CUSTOMER-CENTRIC PRIVACY PRINCIPLES FOR THE BANKING SECTOR .....</b>	<b>47</b>
Segregating Personal Data and Ensuring Visibility Over Personal Data.....	50
Communicating Effectively with Customers .....	53
Obtaining Informed Consent from Customers .....	57
Collecting Accurate and Proportionate Personal Data for Providing Banking Services .....	61
Securing Customers' Personal Data .....	64
Using or Disclosing Personal Data with the Consent of the Customer for Clear, Specific and Lawful Purpose .....	68
Enabling Customers to Access and Rectify their Personal Data .....	72
Using Automated Means of Processing Responsibly.....	75
Demonstrating Compliance with Best Data Protection Practices.....	79
<b>6. SELF-ASSESSMENT CHECKLIST .....</b>	<b>83</b>
<b>7. REFERENCES .....</b>	<b>101</b>

# 1 ABOUT THIS GUIDE

The rapid development of digital technologies and increasing use of the Internet has transformed business models across sectors. Service providers are increasingly employing new technologies to create new consumer experiences. They are also using such technologies to track and profile consumers and collect their personal data. It has become increasingly necessary to examine how the privacy and personal data of consumers can be ensured. This will be necessary to establish consumer trust.



This guide focuses on the banking sector in India. It has been developed as part of a wider project of the Data Security Council of India to develop sectoral privacy guides for key sectors in India that are rich in consumer data (see Figure 1). The aim of this guide is to help participants in India's banking system move closer to adopting a privacy-preserving approach. It is intended for privacy and security leaders and professionals to implement privacy management programs in the banking sector. It will also be useful for personnel who handle consumer data on a daily basis or for senior leadership in-charge of overseeing a framework for personal data protection.

This guide has two major components:

1. A set of privacy principles
2. A self-assessment guide

These have been designed with a “customer-centric” perspective in mind by mapping out a consumer's journey in the banking sector and pairing them with a review of current and emerging regulatory requirements of relevance.



This guide has been created with the assistance of an advisory group of industry experts consisting of Ms. Shilpa Kumar, Partner at Omidyar Network India, and Mr. Rahul Rajendraprasad, Deputy Vice President and Data Privacy Officer at HDFC Bank Limited.

## THE DSCI SECTORAL PRIVACY PROJECT

Since its inception in 2007, Data Security Council of India (**DSCI**) has driven the development of industry standards, best practices, and initiatives on data privacy in India. DSCI has also consistently engaged with policymakers to develop laws and policies to strengthen the privacy and security culture in India. This includes the (Draft) Data Protection Act of 2021 (DPB 2021) and the (Draft) Digital Personal Data Protection Bill of 2022 (**DPDPB 2022**).

A recurring theme during our work on the above draft laws was the need for deep-dives on data-privacy issues in specific sectors rich in personal data. This gave rise to our sectoral privacy project which is an effort to create sectoral guidance for organisations at all levels to understand and apply data privacy standards in their sectoral context. Three sectors were picked to start with: health, insurance, and banking.



## 2 INTRODUCTION



## AN OVERVIEW OF THE BANKING SECTOR IN INDIA

### Banking services help customers manage their finances.

Banks provide banking services in four fundamental ways:

#### 1. Banks accept deposits from customers with the promise of safekeeping.

This function helps customers save their money in the form of deposits. Customers who want to deposit money in a bank need to open an account with that bank. To do so, customers must submit personal information to verify their identity and comply with 'Know-Your-Customer' (KYC) requirements.

#### 2. Banks lend credit to customers in need of money.

They use customers' deposits to advance loans to customers looking to borrow money ('Borrowers'). However, before doing so, banks must undertake thorough risk assessments to ensure that the borrower can repay. Repayments from borrowers help banks recover customers' deposits against which the loans were advanced. The interest earned by banks by disbursing loans is a key source of revenue.

#### 3. Banks help customers make payments to each other through formal payment and settlement systems.

Banks provide a bouquet of payment options including paper-based payments (cash and cheques) and digital payments through mobile phones, internet portals or ATMs.

#### 4. Banks are also important vehicles of monetary policy.

They transmit the central bank's monetary policy stance through the interest rates they pay to the customers on their deposits.

The services banks are offering are expanding with increasing disintermediation in financial services. For instance, banks are also offering other financial products and services, like mutual fund deposits, insurance etc. to customers. Banks are doing this not only directly but also through Non-Banking Financial Companies (NBFCs) and Technology Service Providers (TSPs) who provide channels for providing different financial services. This report groups banks, NBFCs and TSPs together, referring to them collectively as Banking Sector Participants (BSPs).

### The banking sector is strongly regulated.

The conduct of banking services can have strong repercussions on customers and the financial system. Poor banking practices can harm customers' well-being and pose risks to financial stability. That, in turn, can have an adverse effect on public interest and economic growth. Countries therefore have in place frameworks for licensing banking activity and regulating banking activity through prudential norms and conduct norms.



## **The Reserve Bank of India (RBI) regulates the banking sector in India.**

The primary legislations through which the RBI regulates the sector include the Reserve Bank of India Act of 1934 (**RBI Act**) and the Banking Regulation Act of 1949 (**BR Act**).

## **The RBI has a mandate to protect customers, foster inclusion, and safeguard systemic stability, as per these statutes.<sup>i</sup>**

The RBI has the power to frame regulations and notifications and issue guidance towards implementing its mandate. The RBI's interest in data protection and cyber-security stems from these principles. In fact, the RBI recognises customers' privacy as a right in its Charter of Customer Rights.<sup>ii</sup> Further, the Supreme Court of India recognised privacy as a fundamental right in 2018. This implicates government, its functionaries, and regulators to protect citizens' personal data and safeguarding it from unreasonable encroachments.<sup>iii</sup>

## **There exists a fiduciary relationship between the bank and a customer.**

Information received by the bank from the customer are held by the former in a fiduciary capacity. It is for this reason that such information is deemed to be exempted from disclosure under the

Right to Information Act.<sup>iv</sup> Banks are also generally held to a high standard of integrity to preserve the trust of banking customers.<sup>v</sup> Consequently, in recognition of this fiduciary relationship and the expectation to preserve customer trust, banks are expected to maintain the highest levels of confidentiality with respect to customers' personal information and to incorporate measures to safeguard customers' well-being.

## **The Indian banking sector is characterised by low access and usage.**

The Reserve Bank of India's Financial Inclusion Index suggests that customers' access to financial services has increased significantly since 2017. However, customers' usage of these services is lagging.<sup>vi</sup> This is indicative in the banking sector where, although more than eighty percent of the population has a bank account, a significant number of bank accounts do not see many transactions.<sup>vii</sup> Similarly, the number of customers who have access to formal credit from a bank or NBFC is low. Credit seems to be most accessible to customers who have well documented credit history; leaving out non-urban residents, women and low-income earners who lack similar access to formal financial services.<sup>viii</sup> Though digital payments are surging, with transaction volumes exceeding 7,19,797 lakhs in May 2022, it is unclear if they are also being taken up by traditionally marginalised customers.<sup>ix</sup>



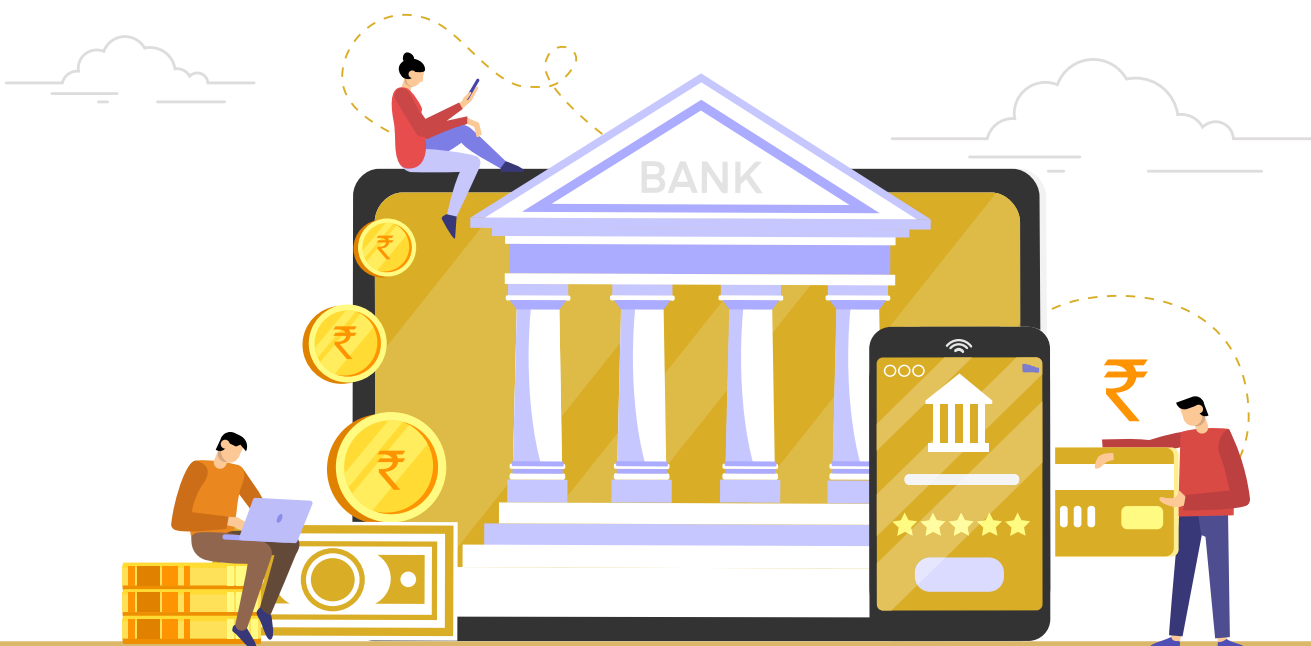


## DIGITISATION IN INDIA'S BANKING SECTOR

**The history of digitisation in banking services dates to the decade between 1980 and 1990.** The path towards digitisation was laid by the Rangarajan Committee which sought to computerise banking in India to make it more efficient. The Committee recommended some major changes to banking services in India. Some of these recommendations started materialising promptly. Banks began adopting computers at their branches. Bank branches were interlinked through Local Area Networks (**LANs**) and the internet. Processes to clear and settle cheque-based payments also became more secure through the adoption of MICR codes and encoders.<sup>x</sup>

**Between 1990-2010, the banking sector developed foundational infrastructure for greater digitisation in the sector.**

For instance, more banks began adopting Core Banking Solutions (**CBS**) in their daily transactions. This change allowed banks to develop centralised banking systems which allowed them to service customers remotely without being tied to a physical bank branch. The RBI also established and licensed major digital payment systems including the Real-Time Gross Settlement System (**RTGS**), the National Electronic Funds Transfer (**NEFT**) system, Immediate Payment Service (**IMPS**), and debit and credit card networks.<sup>ix</sup> These systems allowed customers to make and settle large volumes and values of payment more easily. Alongside these technical developments, these two decades witnessed regulatory developments to support digitisation. Some prominent developments include the enactment of the Information Technology Act, 2000, the Credit Information Companies Act, 2005, and the Payment and Settlement Systems Act, 2007. Among other aspects, these statutes created a data protection and security framework that banks must follow while performing their functions.<sup>xii</sup> The RBI also established the National Payments Corporation of India (NPCI) in 2007 to foster innovation in payment services.<sup>xiii</sup>

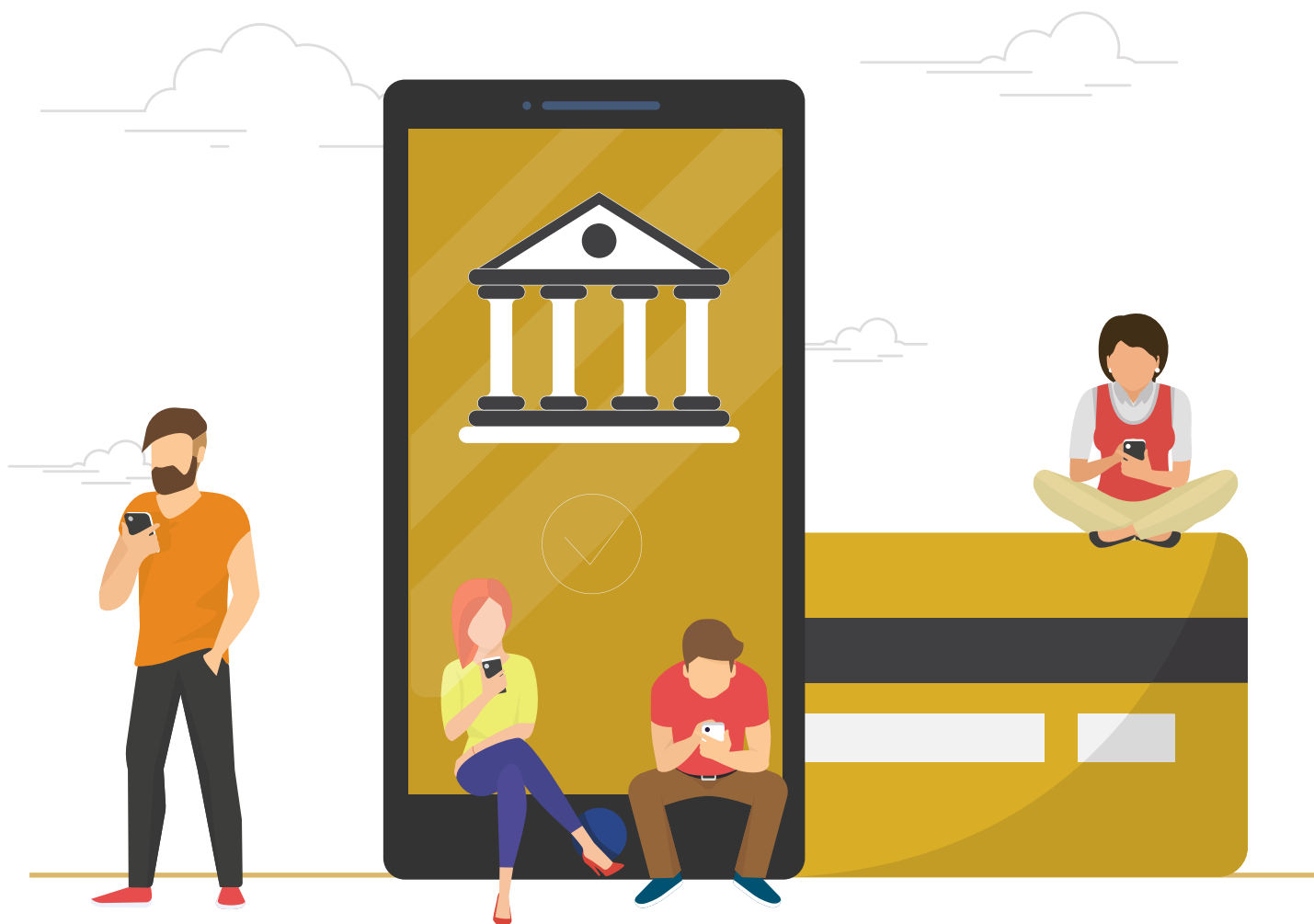


**The foundational infrastructure paved way for more sophisticated banking services to develop between 2010 and 2022.**

This was further supported by the creation of large scale public digital infrastructures like the Aadhaar repository, Central-KYC (**CKYC**) registry, Central Registry of Securitisation Asset Reconstruction and Security Interest of India (**CERSAI**), Unified Payments Interface (**UPI**) and IndiaStack Application Programming Interfaces (**APIs**), that paved way for innovation in the banking sector. These innovations have been focussed towards making banking services seamless and accessible for customers.<sup>xiv</sup>

**Today, mobile phones and other digital devices are becoming major channels for delivering banking services.<sup>xv</sup>**

More banks are providing complete banking services through mobile applications and point-of-sale (**POS**) terminals. The Government is also leveraging mobile banking to provide digitally enabled banking services at the last mile through the Pradhan Mantri Jan Dhan Yojana and the Jan Dhan-Aadhaar-Mobile connectivity (**JAM**) trinity.<sup>xvi</sup> The payments space has especially seen much change with the development of a bouquet of mobile phone-based digital payment services including UPI applications, Pre-paid Payment Instruments (**PPIs**) and Payments Banks (**PBs**).<sup>xvii</sup>



## CHANGES IN THE BANKING ECOSYSTEM DUE TO DIGITISATION

### Digitisation is leading to more disintermediation in banking services.

More non-financial entities, mostly those with expertise in technology services, are entering the banking value chain. These entities are ‘unbundling’ financial services i.e., providing highly specialised and standalone services to intermediate banking services.<sup>xviii</sup> For instance, while payments are primarily the remit of banks, technology providers like card networks and mobile payment applications are entering the value chain to facilitate the payment process. Similarly, while credit scoring is primarily the remit of credit bureaus, banks and NBFCs are relying on technology service providers for alternative credit scoring services.<sup>xix</sup> Technology providers are now also providing highly sophisticated customer-facing digital interfaces for banks. These interfaces, usually offered through mobile apps, are being termed as ‘Neo-banks’ in the Indian context.<sup>xx</sup>

### At the same time, digitisation is allowing greater convergence in banking services.

Digitisation is allowing banking services to converge service delivery processes onto certain channels.<sup>xxi</sup> For instance, competing banks are offering their products over the same marketplace or mobile applications. Similarly, banks are collectively relying on public digital infrastructure to deliver different services. For instance, banks rely on the UPI platform for providing payment services, the Account Aggregator (**AA**) framework for simplifying lending services, and the Central Identities Data Repository (**CIDR**) (or the Aadhaar database) for simplifying Know Your Customer (**KYC**) services.<sup>xxii</sup>

### Providers collect large amounts of personal data from customers.

The increasing use of digital technologies is rapidly increasing customers’ data trails across market segments. This is making it possible for providers to collect and analyse vast amounts of data to draw insights about customers. These insights are proving to be useful for providers in underwriting, distribution, customer segmentation, and other decision-making activities. The data being collected by providers can be of two broad categories –



#### Personal data collected directly from customers:

Providers are by law required to collect some personal data from customers (like the customers’ name, address, and official government identity information) to fulfil KYC requirements. Providers may ask for other kinds of personal information to provide different services. For instance, providers may collect financial asset information or alternative information like call log data if they deem it necessary to provide a loan.<sup>xxiv</sup> Providers may collect personal data directly from customers, or through an intermediary (like a consent manager) that facilitates data sharing. Data collected directly from customers can also include data that providers derive or infer based on customers’ usage of their services. For instance, providers may process data about transactions that customers make using the providers’ facilities.



### **Personal data collected indirectly from third parties:<sup>xxv</sup>**

Providers may collect information about customers from third parties. In a traditional banking sector, this could manifest as providers collecting credit information from credit bureaus. In a disintermediated and platformised banking sector, providers may collect data from different parties including alternative credit scorers and retail merchants selling products and services on the providers' platforms.

Providers may use the traditional and alternative data collected through these channels to assess a customer's needs and provide relevant services. The most common use-case may be to assess a customer's creditworthiness to offer a loan product.<sup>xxvi</sup>



### **Providers are using new technologies to provide banking services.**

Providers are beginning to rely on highly sophisticated technologies for processing personal data, including automated means of processing using Artificial Intelligence (**AI**), advanced big data analytics and distributed ledger techniques.<sup>xxvii</sup> While these technologies power the innovation and operations of digital banking service providers, providers must be conscious of the challenges these technologies can pose.<sup>xxviii</sup> For instance, using automated means of processing may help providers process larger amounts of data and generate outputs more quickly. However, the functioning of the algorithm may be opaque to the providers along the value chain. Regulators and customers may find it difficult to understand the rationale behind a decision made by the algorithm. As a result, providers may be unable to explain why the algorithm generated a particular output. Challenges like these can be highly problematic in cases like lending where exclusionary or discriminatory outputs can adversely affect customers' interests.<sup>xxx</sup>



## THE ROLE OF DIGITISATION IN THE BANKING SECTOR

### Digital banking services have the potential to provide accessible and suitable services.<sup>xxxvi</sup>

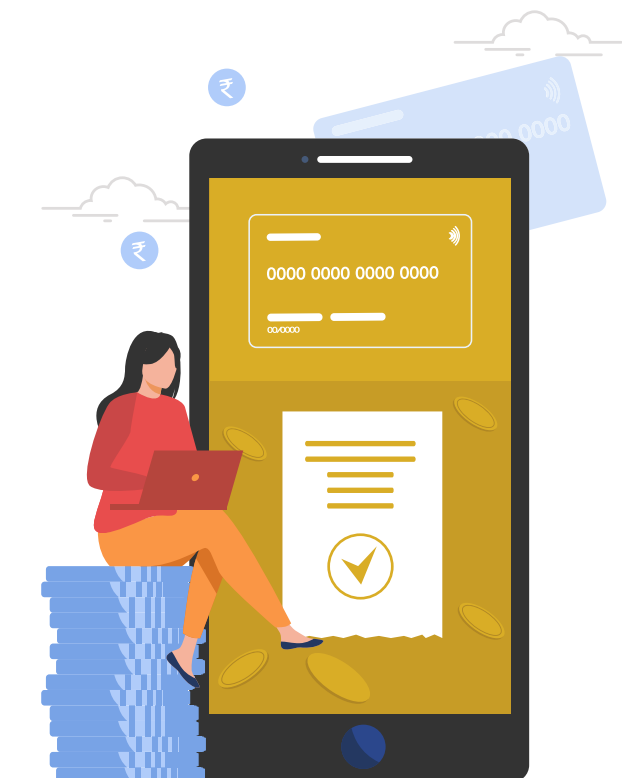
Customers who are excluded from formal financial services are usually excluded because they do not have a prior relationship with the formal financial sector, mainly in the case of credit.<sup>xxxvii</sup> These customers may lack formal credit information records that can help providers assess the customer before providing services. Digital services could promote inclusion and provide customers better access to formal financial products and services.<sup>xxxviii</sup> For instance, providers processing customers' personal data can derive insights that can help providers better understand customers' financial needs and status. These insights can serve as an alternative to credit information, giving customers an entry point to access formal financial services.<sup>xxxix</sup> Further, they may allow providers to provide more products and services that are tailored to the customers' needs and status.<sup>xl</sup>

### Digitisation can foster innovation and make providers' processes more efficient.<sup>xli</sup>

Digitisation can help providers leverage data for innovating new processes and products that can better serve customers. These innovations may also help providers make their processes more efficient.<sup>xlii</sup> For instance, open banking and account aggregator frameworks help customers easily share their data with providers in exchange of aggregated financial services. Providers can benefit from the frameworks by spending fewer resources on collecting that data anew. Similarly, digital banking applications allow providers to deliver the complete suite of banking services without having physical branches that can be expensive to maintain. Innovation and efficiencies generated by digital service providers can in turn help them grow quickly and acquire more customers.<sup>xliii</sup>

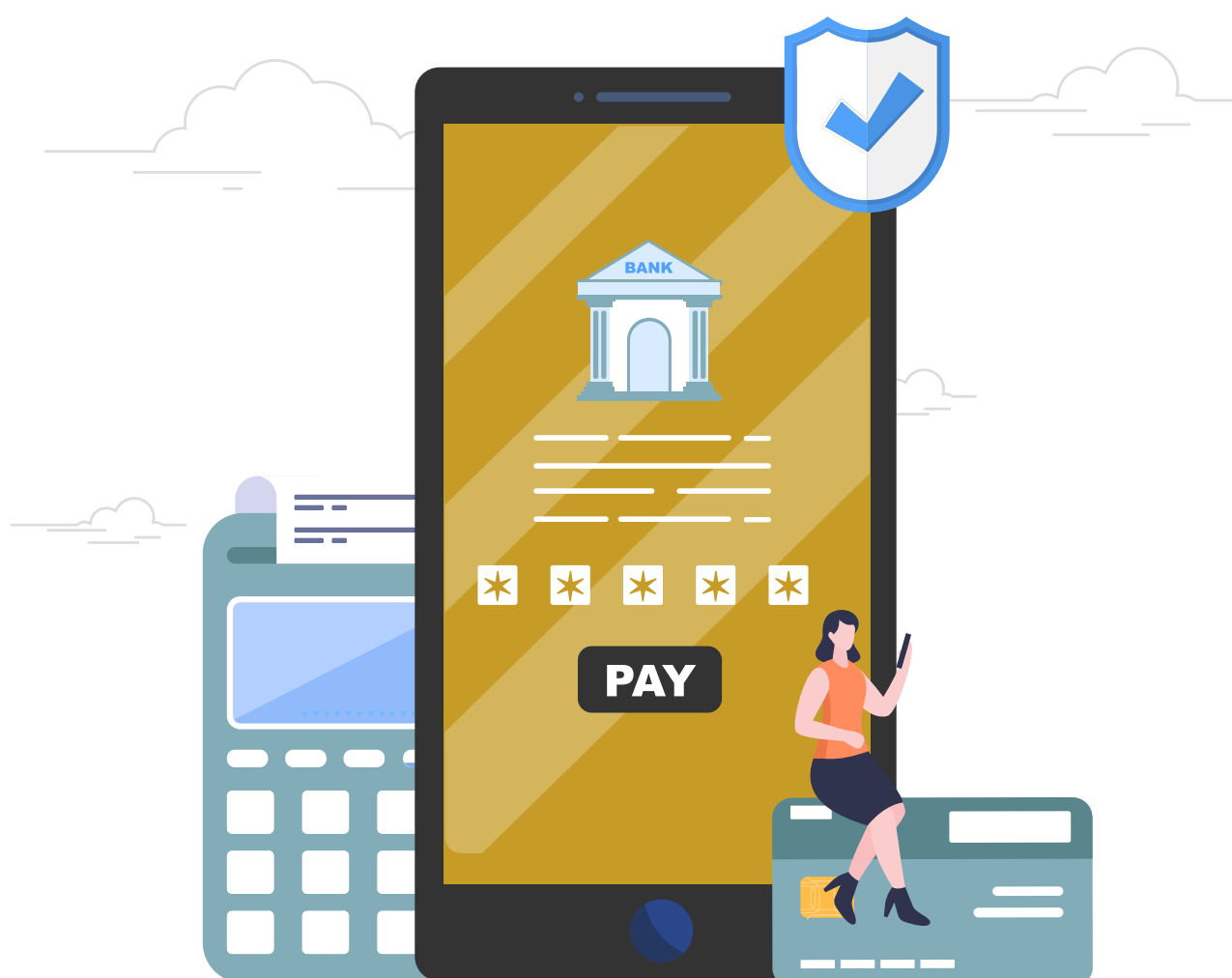
### Providers are offering a suite of financial services, and the RBI is taking note.

Digital payment applications and mobile banking applications have created a gateway for customers to access other financial products. Providers are offering customers near seamless access to a suite of financial products and services, including payments, credit, savings, insurance and investment products, credit information retrieval and financial management services.<sup>xliiii</sup> The RBI is also actively supporting some of these developments. For instance –



- In April 2022, the RBI released guidelines for commercial banks operating Digital Banking Units (**DBUs**). DBUs are meant to help providers deliver financial products and services and help customers to execute financial transactions through digital channels.
- The first two cohorts of the RBI's regulatory sandbox aimed to examine and authorise innovative retail payment products that could (i) facilitate digital payments through Near Field Communication (**NFC**) or voice-based technologies, and (ii) simplify cross-border payments and remittances through platforms.<sup>xli</sup>

The banking value chain is becoming more complex with innovation in products, services, and business models. As discussed above, the number of entities, the kinds of entities entering the chain, and the kinds of personal data being used by providers are all increasing quickly. These developments pose challenges for customers' privacy and data protection.



## POLICY DEVELOPMENTS ON DATA PRIVACY IN THE BANKING SECTOR

### There is increasing emphasis on data privacy in India.

In August 2017, Supreme Court of India, in the landmark *Puttaswamy* judgement, laid down that the right to privacy is protected as a fundamental right under the Constitution of India. The ruling also recognized that this right extends to the protection of personal information. Thus, customers in India are now guaranteed constitutional protection of their data privacy. In the context of financial services, this translates to extending a right to data privacy to all consumers of all financial products and services, protecting them from the unlawful access to their financial accounts by private and public sector entities, and the unlawful disclosure, sharing, or commercial use of their financial information.<sup>xliii</sup>

### A comprehensive cross-sectoral data privacy law for India is expected soon.

Following the *Puttaswamy* judgement, the Ministry of Electronics and Information Technology (**MEITY**), in December 2019, also tabled a draft of a comprehensive data protection law for India called the Personal Data Protection Bill of 2019 (**PDP Bill**) and referred it to a Joint Parliamentary Committee on Data Protection (**JPC**). The JPC tabled its report accompanied by an amended version of the bill entitled the (**Draft**) Data Protection Act of 2021. In November 2022, MEITY released a revised version of the data protection bill, called the Digital Personal Data Protection Bill of 2022 (**DPDPB 2022**), for public consultation. A final iteration of the Bill is expected (**DP Bill**) but its provisions remain to be finalised.<sup>xliv</sup>

### The RBI's focus is steadily widening from confidentiality and data security to data protection.

Most of the regulations in the banking sector currently approach confidentiality from a cyber security and resilience point of view i.e., developing technical security safeguards for digital infrastructure including mobile devices, payment systems and critical payment infrastructure.<sup>xlvi</sup> However, the RBI's emphasis on data protection seems to be strengthening steadily.<sup>xlvii</sup> For instance, the RBI's Master Direction on Account Aggregators emphasises consent, purpose limitation, customer rights over their information and other data protection principles.<sup>xlviii</sup> Similarly, the Guidelines on Digital Lending specify obligations around (i) seeking explicit consent from customers, (ii) collection limitation, purpose limitation, usage, sharing, and storage limitation, (iii) maintaining technology standards, and (iv) creating a publicly available, comprehensive privacy policy.<sup>xlix</sup> The RBI's recent Master Directions on the issuance of credit and debit cards similarly specify customer confidentiality, consent, purpose limitation, accuracy and security as obligations.<sup>1</sup>

### This guide aims to help the banking sector prepare for the future of data privacy law.

At the time of this writing, a draft law is still being reviewed by MEITY. Once a final DP Bill is enacted into law, existing data privacy law across sectors, including in the banking sector, will have to align with the Bill. This guide will aim to help banking sector participants better protect customers' privacy amidst this evolving regulatory environment and increasing adoption of digital technologies in India's banking sector.

# 3 KEY CONCEPTS AND FRAMEWORKS

In this section, we set out certain concepts that are important to understand the rest of this guide and our approach to conceptualising consumer data privacy in the context of the Indian banking system.





**BANKING SECTOR PARTICIPANTS**

We use the term “Banking Sector Participant” (**BSP**) to collectively refer to three categories of entities: *banking companies, non-banking financial institutions and other intermediaries*. Each of these may be further sub-divided as follows

**Banking companies**

Banks may be differentiated on grounds of ownership, and on the nature and scope of their services. Three broad categories are: commercial banks, differentiated banks and cooperative banks.<sup>li</sup> Commercial banks may be further divided into *scheduled* and *non-scheduled commercial* banks:

Scheduled banks include public sector banks (either established by nationalisation laws or having majority government ownership, like the State Bank of India group or regional rural banks) and private sector banks (having majority private sector ownership and including both domestic banks and Indian branches of foreign banks).

- Scheduled banks include public sector banks (either established by nationalisation laws or having majority government ownership, like the State Bank of India group or regional rural banks) and private sector banks (having majority private sector ownership and including both domestic banks and Indian branches of foreign banks).
- Non-scheduled banks include local area banks (small private banks that are limited to specific territories and are set up with the aim of increasing credit availability in rural and semi-urban areas).

*Differentiated banks* are offered narrower licenses than commercial banks and can only provide specific banking services and products.”

There are two main categories:

**Small Finance Banks (SFBs)**

- SFBs are expected to issue small ticket loans and give a majority of their credit to priority sectors (e.g., agriculture, micro-enterprises, housing).

**Payment Banks**

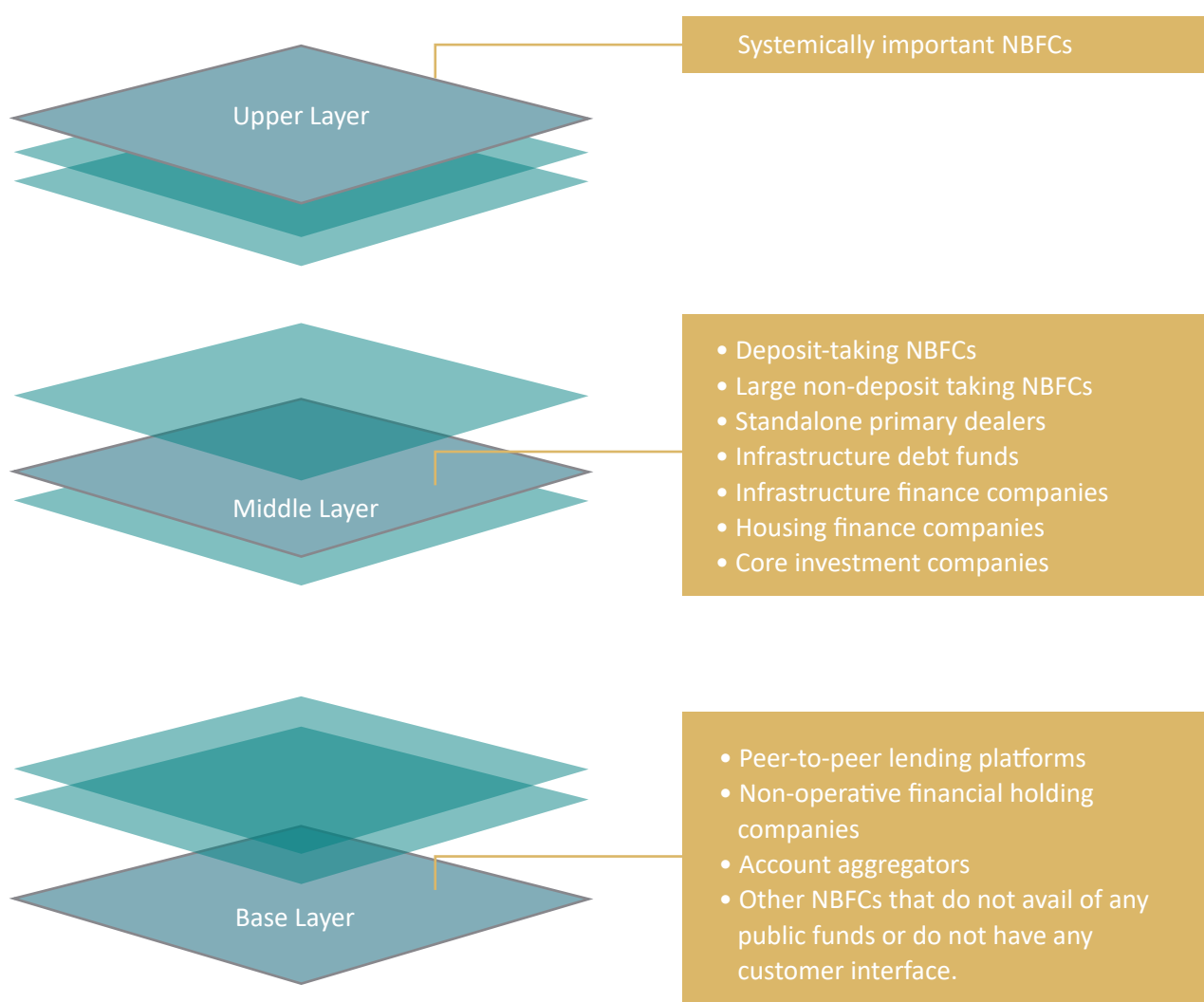
- Payments Banks can accept deposits from customers and provide payment services but are not authorised to give credit

*Co-operative banks* may be divided into *urban co-operative banks, state co-operative banks, and district central co-operative banks*. These are organised under the Co-operative Credit Societies Act of the various state governments.

## Non-Banking Financial Companies

While banks are central to the banking function, they are supported by many intermediaries. Some of the prominent intermediaries include Non-Banking Financial Companies (NBFCs), which are companies engaged in '*purveying credit to key and niche sectors of the economy*'.<sup>lii</sup> The RBI has recently introduced a scale-based regulatory framework for NBFCs, which classifies them into four layers: specifically, the *base, middle, upper* and *top layers*.<sup>liii</sup> While the top layer is currently empty, the NBFCs populating the remaining layers are as follows:

### Types of NBFCs:



Account Aggregators are worth specifically mentioning from a data privacy perspective. These are entities holding a license developed by the RBI following an open banking approach.<sup>liv</sup> They are what the RBI calls “*account information services*” and are exclusively dedicated to collecting, retrieving, and sharing users’ financial information with other financial entities with the users’ consent.<sup>lv</sup> These are conceptually distinct from other NBFCs that are primarily credit providers. As a result, they occupy a unique position in the larger set of NBFCs that RBI regulates.

Before proceeding, we would like to highlight one limitation here. We leave out of scope financial companies that do interface with the banking system but are exempt from the RBI’s licensing or registration regimes and are supervised by other regulators, such as venture capital funds or stock exchanges (regulated by the Securities and Exchange Board of India), insurers (regulated by the Insurance Regulatory and Development Authority) or chit fund companies (regulated by the state governments).<sup>lvi</sup>

### **Additional participants**

Beyond NBFCs, several other intermediaries are also involved in India’s banking system but cannot be regarded as either banks or NBFCs. These include:



#### **CREDIT INFORMATION COMPANIES**

These entities receive a certificate of registration under the Credit Information Companies (Regulation) Act of 2005 (**CIRCA**) to carry on the business of credit information.<sup>lvii</sup> These collect, from banks, lenders and financial institutions, information regarding borrowers’ credit histories, generate credit reports and credit scores on borrowers, and provide these reports to requesting entities. These reports and scores are then utilised by BSPs in their lending activities. Under the CIRCA, these entities are regulated by the RBI.



#### **INFORMATION UTILITIES (IUs)**

These entities are regulated under the Insolvency and Bankruptcy Code of 2016 (**IBC**). They are intended to act as data repositories of financial data which receive, authenticate, maintain, and deliver data pertaining to debts to facilitate insolvency resolution processes. All lenders and banks are required to submit financial data relating to debts and securitised assets held by them to IUs.<sup>lviii</sup> Unlike credit information companies, these are regulated by the Insolvency and Bankruptcy Board of India (**IBBI**) and not by the RBI.



## **PAYMENT SYSTEM PROVIDERS**

This set of entities, most of which are regulated by the RBI as the principal regulator under the Payment Systems and Settlements Act of 2005 (**PSSA**) includes Clearing Corporation of India Limited, National Payments Corporation of India, various cards payment networks, ATM networks and ATM operators, money transfer service providers, issuers of prepaid payment instruments and other payment system operators or service providers.<sup>lix</sup>



## **FINANCIAL TECHNOLOGY OR 'FINTECH' BUSINESSES**

This elastic set of entities consists of newer technology-based businesses that either compete against, enable, interface with, or collaborate with financial companies, including banks & NBFCs,<sup>lx</sup> by developing new technology enabled business models, applications, processes or products in financial markets and services.<sup>lxi</sup> Some FinTech businesses seek to drive financial inclusion through the use of newer technologies, such as mobile banking, paperless lending, or payment gateways. In recent years, several FinTech companies have entered into partnerships with banks and provide branchless access to banking services as well as several other value-added services (e.g., providing customer support, facilitating bank account opening) to customers and, thereby, reach a wider customer segment. These companies are often referred to as “neo-banks” and the bank-fintech partnership is typically structured as an outsourcing arrangement.<sup>lxii</sup> A second prominent model has been “digital lenders”, who use mobile and web applications to facilitate borrowing by consumers from lending service providers.<sup>lxiii</sup> A connected phenomenon driving the growth of the FinTech ecosystem in India is digital payments. Recent innovations aimed at driving cashless transactions, notably the UPI, have seen significant adoption, digitally transforming several payments’ related functions that were traditionally performed by banks in the past and opening a third model of payment wallets and payment service providers to open up for the FinTech ecosystem.<sup>lxiv</sup>



## **ADDITIONAL INTERMEDIARIES**

Banks may often rely on or interface with a wide variety of outsourcing and technology service providers, as well as third parties like monitoring, valuation, and verification agencies. These facilitate a variety of activities in the banking value chain. They may also engage third-party retail agents, such as business correspondents or direct sales agents and originators, to provide banking and credit services at locations other than a bank branch or an ATM.<sup>lxv</sup> These perform a variety of services under the supervision of banks, including identifying borrowers, processing loan applications, customer acquisition, lead generation and last-mile servicing.<sup>lxvi</sup> FinTech businesses have increasingly started providing such services as well.

## KEY DATA PRIVACY CONCEPTS

### Anonymisation

A process of stripping or disguising information from datasets that can be used to identify individuals. It is used to prevent individuals from being identified either directly or by deduction.<sup>lxvii</sup>

### Application Programming Interfaces (APIs)

These are standards, embedded in a set of instructions, that allow software components to interact and exchange data - including over the Internet.<sup>lxviii</sup> APIs can be *internal* or *external*. Internal APIs are those used to connect internal datasets and processes held within an organisation. For example, banks often use APIs to draw data from their servers and display it on the user's phone when the user wants to check their balance.<sup>lxix</sup> External APIs are those used by organisations to let external software interact with their datasets and processes. These can facilitate the creation of 'platforms' held by an organisation atop which third-parties can build applications.<sup>lxx</sup>

### Automated means

A term used in privacy literature and legislation to refer to the use of algorithms and software that use machine learning or other data science techniques to automatically make decisions or suggest information to consumers.

### Collection

A term used to refer to the processes of gathering, acquiring, or obtaining personal data. This is understood as a subset of the concept of processing (see below). Collection includes processes whereby customers provide data about them to BSPs directly (for example, when the customer is completing a Know-Your-Customer (KYC) process, or using a financial product or service, or raising a customer service request or grievance) as well as when data about customers is collected by BSPs from third parties (such as from credit bureaus) or from publicly available information (such as from social media).

### Consent

A term used to refer to the permission that is granted by a consumer to any BSP to collect and process their personal data. Data protection laws often require consent to be 'freely-given' and 'informed', that is, consumers must not be compelled to give such consent and, before giving such consent, they must understand: the intended purpose of the collection or processing; the entities to whom their personal data may be shared; and any risks to their privacy, financial or legal status that may arise from their data being collected and processed.

## Data

A term used to refer to a collection of pieces of information that has been gathered by some means and then converted into a form that makes it possible to store, share or process information efficiently. Digital data refers to data that can be stored, shared, or processed through a computer system. The concept of data may be further divided into structured (data that is consistently structured according to a tabular or relational model) and unstructured data (text, images, audio, video, and relationship data).<sup>lxxii</sup>

## Disclosure

A term used to refer to any process that involves making personal data available to a third-party or outside an organisation. In the past, banks have been held liable for disclosing personal data to unauthorised persons. For example, in 2008, a bank was held liable for disclosing a duplicate passbook of a consumer to their partner without proper authorisation and without following proper procedure on the issuance of a duplicate passbook. This was considered to be a violation of the confidentiality commitment owed to the consumer by a national consumer court. The bank was ordered to provide compensation to the consumer.<sup>lxxiii</sup>

## Notice

A privacy notice is a public statement made by a BSP that explains how they collect and process personal data. Several banks in India upload privacy policies on their websites that act as such notices.

## Personal data

Any information relating to an individual that identifies them or can be used to identify them. Individuals can be directly identified from data such as their names, contact details, or identification numbers and may be indirectly identified from data that describes their recognisable attributes, such as their physiological, physical, behavioural, economic, or sociocultural characteristics. A simple example of personal data in the context of the banking sector are customers' savings accounts, loans accounts, debit, or credit card numbers. These are considered to be rich repositories of important identifying information about individuals (such as their purchases, net worth, donations to religious or political causes, etc.). For this reason, personal data being used by BSPs is generally considered to be especially significant from a data privacy perspective. As we discuss below, financial information is considered as a special sub-category of "sensitive personal data" in current and emerging data protection laws in India.

## Processing

An umbrella term used to refer to a wide range of operations that may be performed, either manually or through automated means, on personal datasets. A non-exhaustive list of such operations includes collection, storage, disclosure, retrieval, organisation, use, publication, destruction, or erasure of data. Some simple examples in the banking sector include sending promotional emails, updating passbooks, copying customer identification documents, analysing customers' credit data, disclosing customers' transaction records to third parties for risk analysis, etc.

## TRACING THE JOURNEY OF THE BANKING CONSUMER

A starting point to addressing data privacy risks and challenges is to determine how and when customers interact with BSPs and provide personal data to them. To do so, we adapted the methodology of *customer journey mapping*<sup>lxxiv</sup> to map out the typical journey of a customer in the banking sector for (i) opening a digital bank account and (ii) purchasing an unsecured digital loan. After reviewing literature on mapping the banking value chain<sup>lxxv</sup> and incorporating insights from our discussions with stakeholders, we provide two customer journey maps in Figures 4 and 5 below. Additional steps may be involved for different banking products.

### Customer journey for opening a new bank account as a retail customer

Figure 5 illustrates the customer journey for opening a new bank account as a retail customer. We assume that the customer opens the account online by accessing a website or mobile application offered by a bank or a FinTech company that facilitates account opening and completion of KYC processes. With this in mind, we have identified the following steps:

#### Search:



A customer may look to open a bank account to fulfil a financial need, such as the desire to store one's savings safely or to use the account to receive governments benefits.



BSP may also proactively solicit customers to open new bank accounts through targeted messaging or other channels of solicitation.



In recent years, several customers have applied for (and received) accounts under government schemes, such as the Pradhan Mantri Jan-Dhan Yojana program.



The customer may receive a list of available banks with whom they may open an account, either by going to different banks' branches in their locality, visiting different banks' websites or mobile applications, or by receiving recommendations from different banks' agents or intermediaries or from friends and family.



## Selection:



As part of the selection process, after settling on a particular financial service provider, the customer would also collect information on the different types of bank account available to them and the rates of interest or other features of different options (such as savings, current, or fixed deposit accounts).

## Onboarding:



After selecting a bank and a particular type of account, if the customer is using a website or mobile application to open the account, the customer would, before initializing the process, likely be required to provide their consent to the terms and conditions of that website or application. This website or mobile application may be operated by a bank or may otherwise be operated by a FinTech businesses enabling account opening process.

---



Thereafter, the customer would initiate the account opening process, and filling up the account opening form. Many websites and mobile applications have innovated atop the account opening process to simplify the process of filling up account opening forms by creating new interfaces for customers to submit information online.

---



As part of this process, the customer would likely provide several different types of personal data, such as their photographs, name, gender, religion, address, occupation, employment status, as well as the details of their nominees.

---



The customer would also upload their identity and address proofs either by uploading the relevant documents (such as a copy of their Aadhaar or PAN card) and/or by entering in their identification numbers (such as their Aadhaar number or PAN).

---



They would also have to agree to the terms and conditions for account opening set by the bank at this stage which would include declarations that the details being provided by the customer are valid, complete and accurate.





At this stage, the customer may pick between first completing a partial electronic KYC (also known as a paperless or e-KYC process) to open a partial account or completing a full KYC process directly.

- Today, e-KYC processes often involve the service provider verifying the identity and address of the customer by accessing the details of their Aadhaar from the database maintained by the Unique Identification Authority of India (UIDAI) database.
- The completion of an e-KYC process would enable the BSP to set up a “partial account”, which is a bank account that can be accessed by the customer to deposit money and make transactions but is limited by the RBI in terms of deposit and time limits.
- Thereafter, the customer would, to remove these limits and access their account in full, have to complete a full KYC process, which may take place either by directly visiting the relevant bank’s branch in person or by completing a video KYC process being run by the bank or its partner intermediaries.
- Upon the completion of the video KYC process, the BSP may complete other risk assessment and verification processes, such as by requiring the customer to provide references from existing customers of the bank, or by checking the customer’s history against public and private databases or official sources. This may vary across different BSPs and account types.



After the onboarding process is complete, and no concerns are raised during the risk assessment and verification processes, the customer will receive an approval and their bank account will be opened.



The customer would then be required to transfer the minimum deposit required to open the account and maintain the minimum balance required. Banks would also require the customer to submit a specimen of their signature. If these are submitted online, then the specimen may also itself be electronically signed.



The customer will likely then be provided with a welcome kit, including a debit card and a series of disclosures and brochures regarding their account. Thereafter, the customer would start using their account.

## Use:



The customer would then access their account either online or by visiting the bank branch or an ATM.

---



Typical transactions engaged in using bank accounts include receiving amounts, making deposits, payments, remittances, withdrawals, or transferring amounts to others.

---



A customer may also use their bank account to purchase other financial products and services from the BSP providing the bank account, given that they have already completed a detailed KYC process while opening the account.

---



The BSP would be collecting and processing data regarding the usage of the account by the customer, which would include personal data regarding the customers' transactions, such as about their payments, received income, taxes, etc.

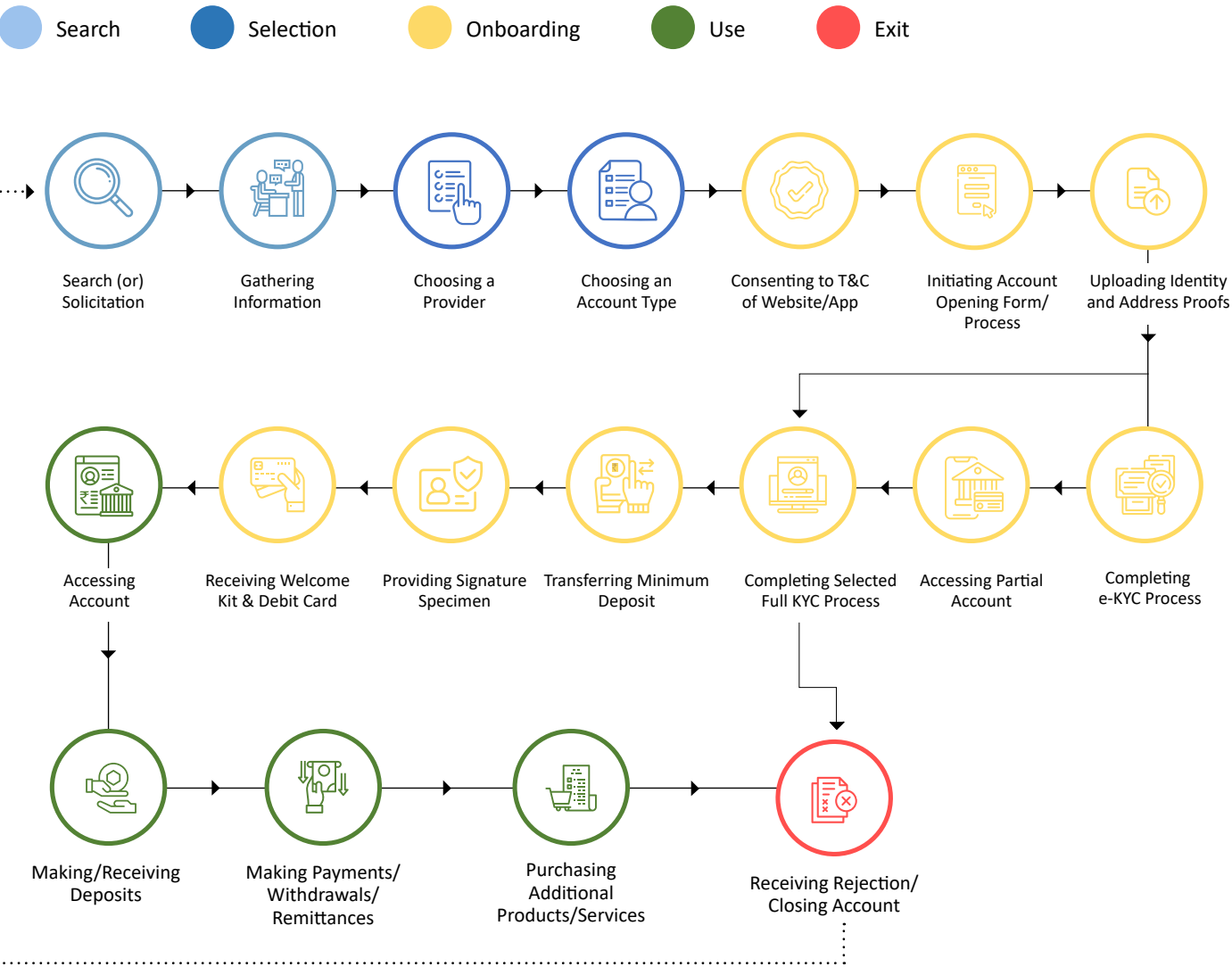
## Exit:



A customer's relationship with a bank regarding a bank account may be complete either when they receive a rejection during the account opening and KYC process, or when the customer closes their account and withdraws their deposit. BSPs may use the existing relationship with customers to again solicit them with other products at a future date.



Figure 5: Customer journey for opening a new retail banking account online



## Customer journey for purchasing an unsecured digital loan

Figure 6 illustrates the customer journey for purchasing an unsecured digital loan. We identified the following steps:

### Search:



This journey of a customer begins after they have identified the need for an unsecured loan. This need could arise because of a life event. For instance, a customer may want to sponsor the purchase of a gadget. Alternatively, a BSP may proactively offer loan to a customer through targeted messaging or other channels of solicitation, such as embedded finance.

---



Next, the customer may gather more information about the product or seek advice on available options and providers. It is to be noted that sophisticated customers are more likely to gather information on competing loan products or comparing them. In this phase, the customer interacts with various banks, NBFCs and intermediaries through online and offline channels. In recent years, banks' websites, digital applications and banking marketplaces have emerged as a key avenue for gathering information.

---



Banks, and a variety of intermediaries [such as Direct Sales Agents (**DSAs**) and originators],<sup>lxxvii</sup> may also collect some personal data from the customer to assess their needs and determine their suitability for a loan.

---



The customer may end up submitting personal data at this stage to a variety of BSPs to receive information and advice such as their contact details, lifestyle habits, income and other financial information.

## Selection:



The customer may receive a list of available options for the desired loan, either from the bank, agents, intermediaries, or through online marketplaces. The customer may make their choice after comparing their features.

---



After selecting the option, the customer will likely fill up an application.

## Onboarding:



The lifecycle of the loan product begins with the submission of the application. At this stage the lender may seek the customer's consent to their terms and conditions, and to collect and process personal data to further process the application. This is a significant step since this will involve consenting to terms of services of the lenders and intermediaries and their requests to process personal data. Lenders may rely on Account Aggregators at this stage to seek customers' consent and access customer's financial information stored with other financial institutions.

---



When a customer gives their consent, they may be sharing large amounts of personal data including –

- **KYC information (name, address, gender, official identification etc.):** Customers may complete KYC processes by giving BSPs consent to access the Central KYC (CKYC) registry, by allowing BSPs to query the eKYC registry (stored with the UIDAI), or by sharing necessary information directly through offline or online channels.
- **Financial information (income, transaction history, outstanding loans, financial assets etc.):** Customers may use the Account Aggregator framework to share this information from other financial institutions, or directly by submitting necessary information.
- **Credit history:** Customers may share their credit history when BSPs query credit bureaus for the customers' records.
- **Alternative information (utility bill payments, mobile phone contacts, SMS logs etc.):** BSPs may be able to collect this information directly from customers based on their consent, or indirectly through third parties.<sup>lxxviii</sup>



The information that customers share with BSPs may be used for customer verification and for assessing their risk profile. Risk assessments help BSPs in making a credit decision about the customer.

---



After the onboarding process is complete, and no concerns are raised during the risk assessment and verification processes, the customer may receive the approval for an unsecured loan from the lender.

## Use:



If a customer's loan application is approved, the customer will have to confirm their purchase by executing the loan contract. This would be followed by the lender providing a loan certificate and disbursing the loan amount to the customer's bank account. Loan certificates may be delivered digitally to the customer.

---



After receiving the loan amount, the customer will be required to repay regular instalments to the lender. These repayments can happen offline through cash or cheques, or digitally through various electronic modes of payment (NEFT, UPI etc.). This may involve the exchange of financial data between the customers and BSPs i.e., the lender, credit bureaus, and any third-party service providers including technology companies involved in facilitating repayments services to the lender. Making repayments regularly will help customers fulfil their repayment obligations.

---



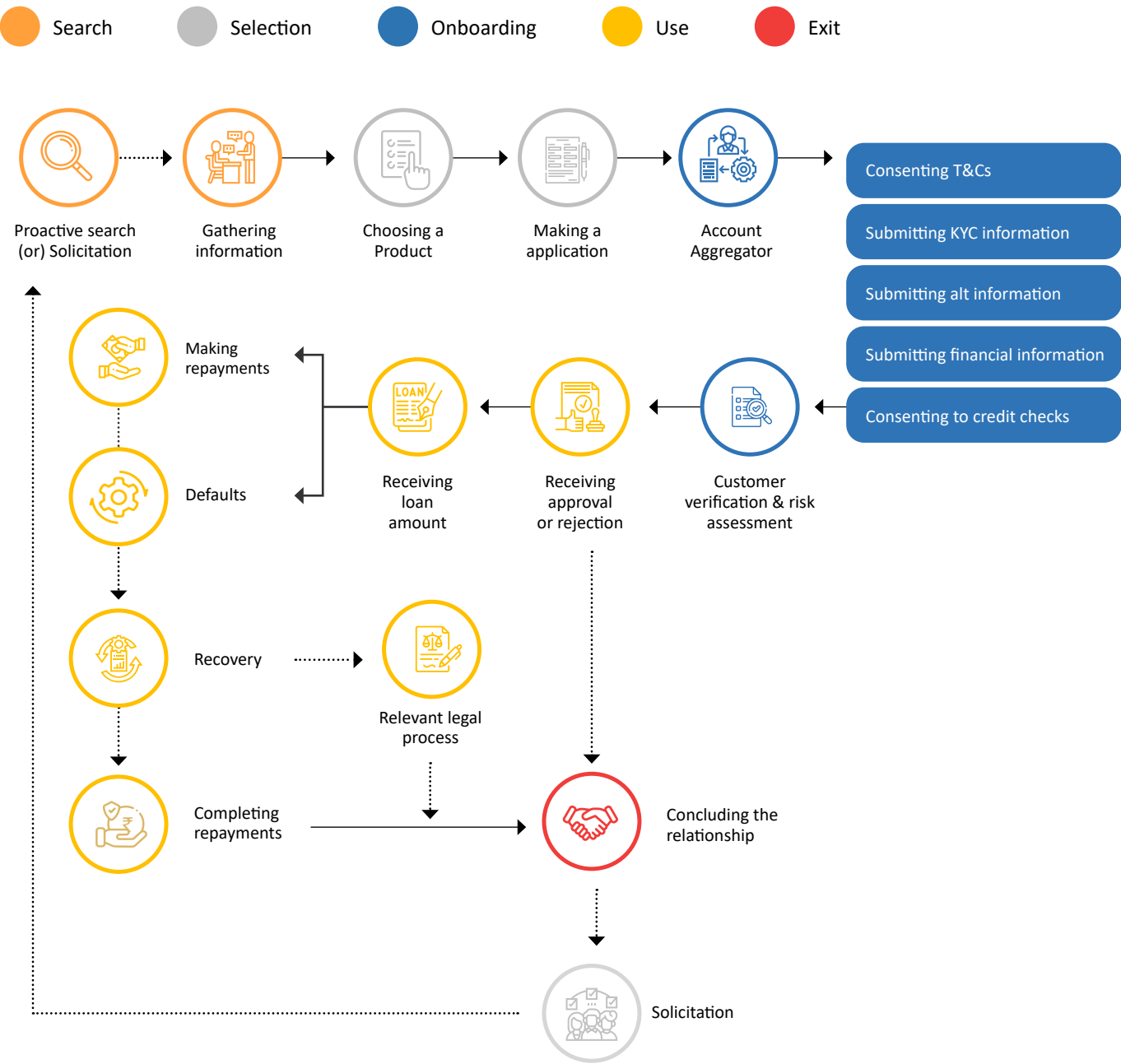
Alternatively, customers may default on making regular repayments to the lender. In this case, lenders may begin recovery processes by engaging recovery agents. Recovery agents would then engage with customers to ensure they make repayments on time. Should customers still default on repayments, the lender may choose to approach the relevant court or forum to initiate recovery proceedings against the customer. The objective of the recovery process is to recover the loan amount the customer had borrowed. Here too, information about repayments made by customers may be exchanged with BSPs including the lender, credit bureaus, recovery agencies and third-party service providers involved in the transaction.

Exit:



A customer’s relationship with a lender may be complete when the lender rejects the customer’s loan application, or when the customer has completed their repayment. BSPs may use the existing relationship with customers to again solicit them with loan products at a future date.

Figure 6: Customer journey for purchasing an unsecured digital loan



## Data flows between customers and BSPs

Throughout the customer journey, customers engage with many entities with whom they share different kinds of personal data. Customers also generate personal data through the transactions they make with the lender. Inadvertently, they may share such transactional data with some intermediaries facilitating the transaction. For example, a customer who makes a payment to a bank may inadvertently share information with their own banking application provider or payment application provider.

Figure 7 below maps the data flow between the customer and BSPs in an unsecured digital lending value chain. In Figure 6 –

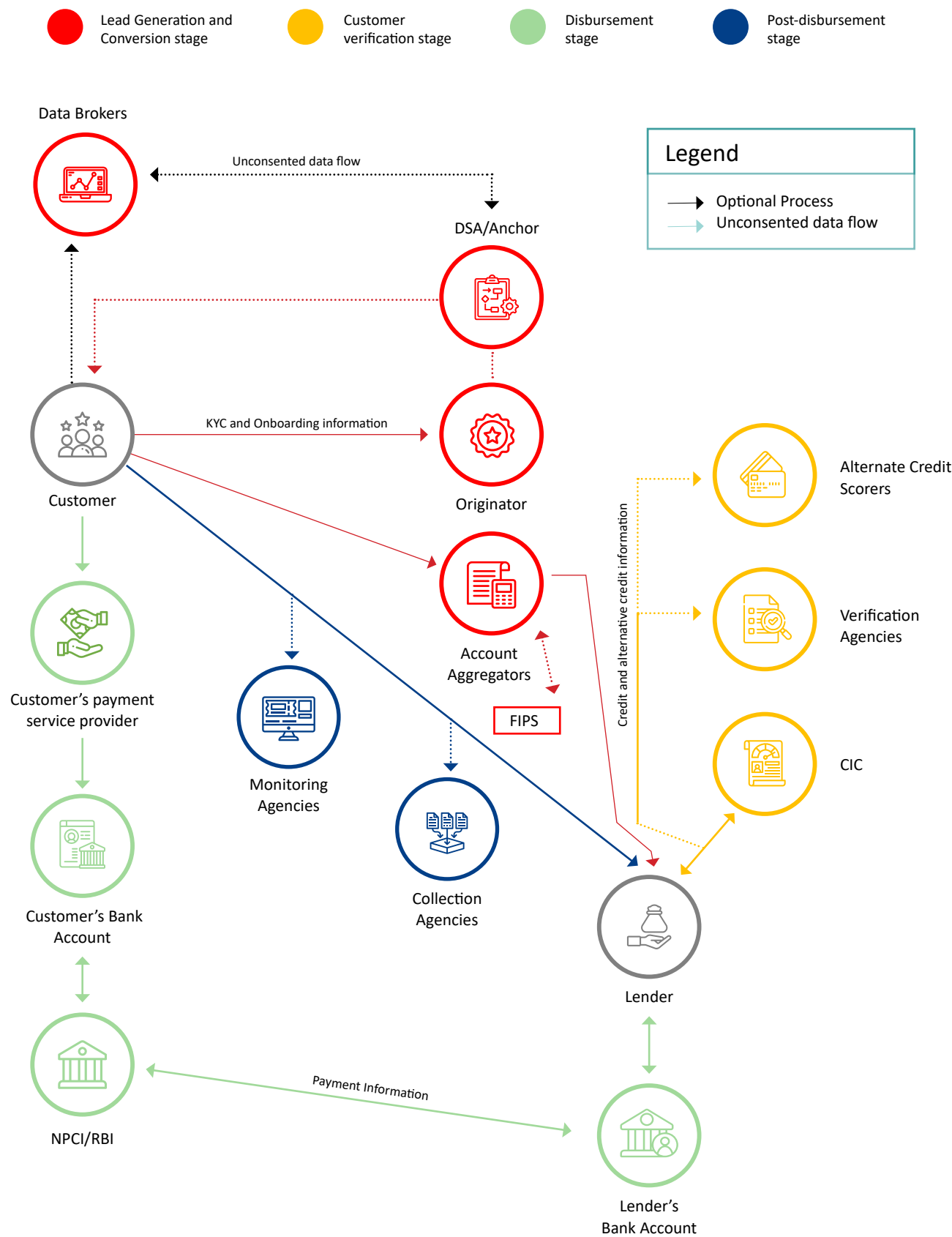
1. ***The lead generation and conversion stage corresponds to the “search”, “selection”, and “onboarding” stages of the customer journey.*** In this stage, customers share personal information including KYC information necessary to make a loan application. This could happen through DSAs and Originators which generate leads for lenders. It is possible that these lead-generating entities may rely on third-party data brokers for identifying potential customers, perhaps without the customer’s consent. Customers may also share financial information with lenders through the Account Aggregator framework.
2. ***The customer verification stage corresponds to the “onboarding” stage of the customer journey.*** In this stage, lenders verify customers and perform lending risk assessments based on

(a) information submitted by the customer, (b) credit information from credit bureaus, and (c) alternative credit information from alternative credit scoring entities (usually technology service providers with alternative credit risk modelling abilities).

3. ***The disbursement stage corresponds to the beginning of the “use” stage of the customer journey.*** In this stage, lenders disburse the loan amount to the customer. The payment information generated in this stage may be accessible to the entities facilitating the payment i.e., lender, lender’s bank, payment system operators (NPCI/RBI), customer’s bank account and payment service providers. The DSA/Originator may also be involved in the chain if the customer is interacting with the lender through them.
4. ***The post-disbursement stage corresponds to the “use” and “exit” stages of the customer journey.*** In this stage, customers’ repayments may be monitored by debt-monitoring agencies and collection agencies. Therefore, these entities become privy to payment and personal information that is exchanged between the customer and the lender. Lenders would also report customers’ repayment information to credit bureaus at periodic intervals.



Figure 7: Data flow map in an unsecured digital lending value chain



# 4

## THE CHALLENGE OF CONSUMER PRIVACY IN BANKING



Today, BSPs face a wide range of compliance challenges and risks from a data privacy perspective. We will discuss them in this chapter.



## ENSURING COMPLIANCE WITH EXISTING REGULATIONS ON DATA PRIVACY

As noted in the first chapter, the banking sector is highly regulated. A patchwork of cross-sectoral laws and sectoral regulations already impose several overlapping data privacy obligations on different types of BSPs in India. Relevant frameworks include:



### Cross-sectoral laws:

Currently, the principal cross-sectoral law on data privacy, that applies to all private sector entities (including any BSP), is a set of rules prescribed under section 43A of the Information Technology Act of 2000 (**IT Act**). Specifically, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**SPDI Rules**) set out general practices and requirements, including the need to publish a privacy policy, collect consent before collecting personal data, appoint personnel to handle complaints, or to adhere to recognised data security standards (such as the ISO/IEC 27001).

The SPDI Rules, however, only apply to certain categories of “Sensitive Personal Data or Information” (**SPDI**). In the context of the banking sector, the primary category of SPDI of relevance is ‘financial information’. This includes “bank account or credit card or debit card or other payment instrument details”.<sup>lxxix</sup> Given that such information is handled regularly by BSPs, the SPDI Rules would apply to BSPs. The IT Act does set out penalties for violating SPDI Rules – specifically, any entity that is determined by a specialised quasi-judicial authority (‘adjudicating officers’) appointed under the IT Act to have violated the SPDI Rules may be ordered to pay compensation to the consumers impacted by the violation.

In addition to the SPDI Rules, other cross-sectoral laws concerning specific types of information apply to processes and activities in banking which concern such information. A key example is the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act of 2016 (**the Aadhaar Act**), which governs how banks can access and use Aadhaar information from the CIDR for e-KYC.



**Financial laws:**

While cross-sectoral laws would impose data privacy obligations on BSPs by virtue of applying market-wide, it is worth noting that, since bank accounts constitute highly sensitive information of customers, a legal obligation specifically applicable to bankers to ensure customer confidentiality has existed under common law long before modern data protection laws were conceived. The scope and boundaries of this obligation were definitively laid down in 1924 by the Court of Appeal of England, when they held that, firstly, bankers owed a duty of confidentiality to a customer and, secondly, banks could only disclose a customer’s financial information in four scenarios:

	Under legal compulsion		From a duty to the public
	To protect the bank’s interest		By the express or implied consent of the customer

These were to prevent banks from sharing consumers’ confidential bank account details indiscriminately.

In India, this common law principle has been upheld by courts<sup>lxxxix</sup> and also embedded into legislations applicable to the banking sector, including State Bank of India Act of 1955,<sup>lxxxix</sup> Regional Rural Banks Act of 1976,<sup>lxxxix</sup> or Banking Companies (Acquisition and Transfer of Undertakings) Act of 1980.<sup>lxxxix</sup> These laws require bank employees, auditors, and advisers to sign declarations of fidelity and secrecy to not “*divulge any information relating to, or to the affairs of, its constituents*” except when required by law or standard industry practice.

These general obligations are complemented by more specific legislations applicable to specific types of financial information, such as credit and payment information. Under the Credit Information Companies (Regulation) Act of 2005 (**CICRA**), which codifies the credit information framework and empowers the RBI to regulate the credit information ecosystem, banks are entitled to receive credit information, but must ensure they take steps to implement certain privacy principles, when ‘*processing, recording, preserving and protecting the data relating to credit information*’ and security safeguards to ensure that the data relating to the credit information maintained by them is “*accurate, complete, duly protected against any loss or unauthorised access or use or unauthorised disclosure thereof*”.<sup>lxxxv</sup> The CIRCA is also reinforced by specific provisions in the RBI Act, which state that any credit information must be treated as confidential and shall not be published or otherwise disclosed, except when required by the law, RBI or other standard industry practice.

Under the Payment Systems and Settlements Act of 2007 (**PSSA**), which gives RBI the power to authorise and regulate payment and settlement systems, all providers of payment systems are required to keep all information provided by 'system participants', except when required to disclose such information under law, or with the consent of the system participant.<sup>lxxxvii</sup> Such information may include personal data of consumers, making this obligation relevant from a data privacy perspective as well. It is worth noting that the RBI has used its powers under the PSSA to introduce data localisation obligations on payments data; these apply to all transaction details and information collected as part of payment instructions and would, therefore, extend to any personal data captured within this category of data.<sup>lxxxviii</sup>

Under the Insolvency and Bankruptcy Code of 2016 (**IBC**), which provides the framework for the registration and regulation of Information Utilities (**IUs**), all IUs are required to meet several duties concerning customer privacy, including ensuring that they adopt secure systems for information flows, provide services based on explicit consent, enable the portability of information submitted by users, and generally protect their data processing systems against unauthorised access, disclosure, alteration or destruction. When providing a functionality for their users to access information stored with another IU, the IU is required to ensure that the functionality ensures privacy and confidentiality of information.<sup>lxxxix</sup>





### Sectoral regulations:

The RBI has specifically recognised the importance of privacy in the context of the banking sector. In 2014, the RBI introduced a “Charter of Customer Rights” which included, amongst other rights, the right to privacy. It required all financial service provider (including any BSP) to ensure that customers’ personal information is kept confidential unless

- 1) They have specifically consented to any disclosure
- 2) The information is required to be provided under the law or
- 3) It is provided for a mandated business purpose (such as to credit information companies).

Customers must be informed upfront about likely mandated business purposes and shall have the right to protection from all types of communications which infringe upon their privacy.

Apart from the above Charter of Customer Rights, the RBI has also put in place several regulations and guidelines that impose obligations on various BSPs and contexts with the aim of ensuring customer privacy and confidentiality.

Here is a snapshot of the relevant sectoral regulations specified by the RBI, as applicable on different BSPs.



**BSP****Data privacy and associated requirements****All RBI-regulated entities offering a digital payment product or service<sup>xc</sup>**

- Expected to formulate a policy for any digital payment products and services that should discuss (amongst other requirements) how they shall protect the confidentiality and integrity of customer data.
- Expected to put in place internal control systems to give effect to the above policy.
- Expected to conduct both internal and external risk assessments of digital payment products and services that shall consider, amongst other risks, the protection and security of payments data and customer privacy.
- Expected to maintain a database of all systems and applications storing customer data.
- Expected to ensure that customer information (including account numbers, card numbers and other sensitive information) is redacted or masked when transmitted through SMS or e-mails by the regulated entity.
- Expected to ensure that digital payment applications, products and services follow a security-by-design approach.
- Expected to ensure mobile applications do not store or retain sensitive personal or consumer authentication information. Sensitive information in 'temp' files must be limited and, in all instances, information in such files must be encrypted or masked or hashed and stored securely.
- Expected to follow standards on payment card security prescribed by the Payment Card Industry (PCI), to ensure that no card details are to be stored in plain text and the processing of card details through readable format must be performed in a secure manner to avoid data leakage of any sensitive customer information.
- Expected to ensure that end-users are educated about safe and secure transactions using digital payments.



### **All RBI-regulated entities during customer onboarding<sup>xci</sup>**

- Expected to ensure that consent is recorded in an auditable and alteration proof manner during the onboarding process of the customer using video e-KYC methods.



### **Banks<sup>xcii</sup>**

- Expected to withhold customer information arising out of the contractual relationship between the banker and the customer from third parties except under some circumstances, when it is required by law.
- Expected to ensure that information collected from consumers for opening their accounts is treated as confidential and not divulged from cross-selling or other purposes without the explicit permission of the customer.
- Expected to ensure that information collected for account-opening is relevant to the perceived risk and not be intrusive. Any other information that may be used for other purposes from the customer should be sought separately with his/her consent and after opening the account.
- Expected to classify data/information on classification/sensitivity criteria of the bank and to protect data/information, both at rest and in-transit, by providing secure access to the bank's assets and services.
- Expected to protect customer access credentials against leakage and attacks, keep customer identity information secure, and develop a data loss/leakage prevention strategy to protect business and customer data and information.
- Expected to understand that any requests from government agencies to collect information will not be of such a nature that the laws relating to secrecy in banking transactions will be violated.
- When issuing any credit card, expected to ensure that unsolicited cards are not issued, and consent for issued cards is explicit and written (and not implied). It should also be ensured that:
  - a) credit limits are not unilaterally increased
  - b) unsolicited loans or credit facilities are not offered without consent
  - c) customers are made aware of possible disclosures of their personal information
  - d) customer information is not disclosed without informed consent to other entity.



- Expected to ensure the preservation and protection of the security and confidentiality of customer information in their custody or in the possession of their business correspondents.
- Expected to ensure that personal information issued to any agents is only limited to the extent needed to discharge their duties, and to ensure that the bank is responsible as the principal for all acts of omission or commission of their agents (e.g., recovery agents).
- Endeavour to improve customer awareness and educate them of the many cyber security risks that might occur and the means to protect themselves from such risks.
- Expected to ensure any outsourcing arrangements executed by it should not affect the rights of the customer against the bank. Any such arrangement should incorporate, in the agreement:
  - a) controls to protect customer data confidentiality
  - b) ensure the service provider can isolate and identify the bank's customer information to afford protection for the same
  - c) affix service provider's liability in the case of a breach of security or leakage of confidential customer information and
  - d) customer information should continue to be maintained even after expiration or termination of the contract.



**NBFCs<sup>xcii</sup>**

- When issuing any credit card, it is expected to ensure that unsolicited cards are not issued; consent for cards issued as explicit and written (and not implied); credit limits are not unilaterally increased; unsolicited loans or credit facilities are not offered without consent, and customers are made aware of possible disclosures of their personal information (including to CICs) and that such customer information is not disclosed without informed consent to other entity.
- Expected to ensure that personal information issued to any recovery agents is only limited to the extent needed to discharge their duties. The NBFC will be responsible as the principal for all acts of omission or commission of their agents (e.g., recovery agents).
- Expected to have a robust grievance redress mechanism. The rights of a customer shall not be affected by outsourcing arrangements entered by the NBFC.
- Expected to ensure that an outsourcing agreement shall ensure the confidentiality of customer data and the liability of the service provider in the event of breach of security or leakage of confidential customer information. The agreement shall incorporate a clause that stipulates that even after the agreement expires or is terminated, the confidentiality of the customer's information shall be maintained.
- Expected to ensure the 'preservation and protection' of both security and confidentiality of customer information in its custody and in the possession of a service provider. Staff of the service provider may access the customer information only on a 'need to know' basis. The NBFC shall ensure that the service provider can isolate and identify the NBFC's customer information and data to protect its confidentiality. In the event of a security breach or a leakage of confidential customer information, the NBFC shall notify the RBI.
- Expected to ensure that neither the NBFC nor its agent intrude into the privacy of its debtor's family members, referees, and friends in their debt collection efforts.



### Payment system providers<sup>xciv</sup>

- Expected to ensure that the entire data related to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details/information collected, carried, processed as part of the message/payment instruction.



### Account aggregators<sup>xcv</sup>

- Expected to provide services to a customer only based on the customer's explicit consent.
- Expected to ensure that any financial information of the customer accessed by it from financial information providers does not reside with it.
- Expected to not use/access/disclose any customer information other than for the purpose explicitly consented to by the customer.
- Expected to develop a Citizen's Charter that guarantees protection of the rights of a customer.
- Expected to build adequate safeguards in its IT systems against unauthorized access of records and data.
- Expected to not request or store customer credentials which may be used to authenticate customers to any financial information providers.
- Expected to allow customers to access record of the consent provided by them and a list of the financial information providers with whom their customer information has been shared.



## PREPARING FOR NEW OBLIGATIONS AMIDST RISING DATA PRIVACY RISKS

### **A comprehensive data protection law is expected for India soon.**

As discussed in the previous section, a new DP Bill may soon be passed into law, which will induce a shift in compliance obligations and mechanisms across the banking sector. It will also impact the extent to which BSPs may be able to collect customer data from different sources. The DP Bill will build upon the existing regime to create a more nuanced and customer-centric data protection regime, with a key component being the introduction of new rights for customers in relation to their personal data.<sup>xcvi</sup>

However, at the time of writing, a key overarching concern is the regulatory uncertainty surrounding the DP Bill – it is simply not clear what may or may not be permitted in the final version of the law.<sup>xcvii</sup> Representatives from the banking sector have questioned, for example, if and how the DP Bill will regulate the use of alternative data by credit information companies, BSPs, and other financial sector participants.<sup>xcviii</sup>

We note below specific additional challenges that BSPs may face when transitioning to and complying with the new regime:

### **Building awareness and privacy-focused capabilities.**

The DP Bill will trigger a significant conceptual shift in the regulatory landscape for BSPs. For banks, this will mean transitioning away from an approach to protecting customer information based on a purely “security” or “confidentiality” basis to one that is based on a customer-centric privacy approach, requiring far more than

just ensuring information security. This is not to say that BSPs are unfamiliar with data privacy – in fact, banks have been amongst the few entities against whom the SPDI Rules have been enforced. For example, in 2019, a bank was held liable for negligently disclosing confidential information (such as customers’ passwords) and was required to introduce access control measures to ensure security of customer information.<sup>xcix</sup>

However, the DP Bill will likely introduce new or heightened obligations as compared to the SPDI Rules. For example, the DP Bill will require BSPs to now map out and keep track of why personal data is being collected, from whom, where it is floating within the organization, and to whom it is being discussed. It will also require BSPs to build workflows for consumers to raise requests for their rights in relation to their personal data as guaranteed under the DP Bill. These are all relatively new requirements. Some BSPs may not have data compliance teams to interpret and secure compliance with them and will need to invest in resourcing and building internal capacity around data governance.



### **Introducing processes for consent management for data collection.**

A key concern would be ensuring consumers are provided adequate notice, and further ensuring that they provide, in turn, adequately informed or meaningful consent, before their personal data is collected by a BSP. The DP Bill will require entities, including BSPs, to meet specific legally binding standards of consent and to disclose a wide variety of details about their data processing operations to consumers. It is expected that new business models, such as account aggregators, that have recently been recognised in the financial sector, will play a key role in helping BSPs manage consent.

### **Complying with new transparency and accountability obligations.**

This will be especially important considering the data-intensive nature of the industry. BSPs have historically processed different kinds of personal data. Today, with new sources of personal data and processing technologies, BSPs are processing more and more granular personal data points. For example, banks are processing data from mobile bills and electronic commerce histories to determine customers' creditworthiness.<sup>c</sup> At present, banks may not have in place sufficiently robust or granular data discovery and inventory management systems to distinguish between these different sources of customers' personal data (beyond differentiating between their KYC records and other data) which would be necessary to ensure compliance with the DP Bill. It is likely that BSPs will need to engage in a comprehensive process to adjust to these new regulatory requirements.

### **Adhering to new data privacy principles.**

The DP Bill will also require BSPs to build internal processes and systems to ensure adherence with new data privacy principles, such as lawfulness, accountability, accuracy, or storage limitation. These principles would require BSPs to ensure that they only collect, process, or store personal data to the extent necessary for meeting a lawful purpose that either the customer has provided consent to or to comply with a legal obligation. These will require BSPs to re-organize their activities involving personal data around specific lawful purposes – a new compliance process that many BSPs would not be familiar with at present.

### **Introducing new security and privacy-enhancing safeguards.**

The traditional approach to the security of customer data has been influenced by the RBI's approach which has largely been centered around information security. However, the DP Bill will likely incentivize BSPs to invest in, and adopt privacy-enhancing technologies, like de-identification and anonymization, which may be challenging to incorporate at scale.

### **Managing disclosures to third parties.**

The banking value chain is characterised by a complex mix of regulated and unregulated entities. Today, there can be over 15 to 20 roles for service provision in various stages with multiple vendors filling these roles and, consequently, entering into agreements and arrangements with banks. At scale, it can be extremely difficult for BSPs to monitor

the nature of their control over the data and the extent of their involvement in the processing of personal data in each case. Specific concerns arise from the use of digital technologies to enable third-party data access, such as through the use of APIs. There are often no accepted standards for APIs; risks can arise from poorly designed and insecure APIs. In some cases, it is possible to misuse APIs to mirror and share personal information with third parties without adequate authorisation. There is a scope for a fraud being perpetuated from unauthorised data sharing and the leakage of customer data.<sup>ci</sup> This is exacerbated by the lack of adequate oversight over such APIs. Further, the risk of unauthorised access to personal data by third parties increases as the banking value chain becomes more disintermediated. Such a breach violates customers' privacy over their personal data and also exposes the BSPs to regulatory requirements and potential penalties.

### **Building consumer trust in the wake of digital banking.**

The rise in digital banking can amplify concerns for customers' privacy over their personal data. In particular, the way providers process customers' personal data can harm customers' interests in certain cases. For instance, providers may be unable to fully understand the outcomes of processing personal data using new techniques or technologies (like processing using automated means).<sup>cii</sup> These processing activities may lead to different kinds of outcomes including discrimination, exclusion, and fraud.<sup>ciii</sup> Strengthening relationship of trust between BSPs and customers is very important. Customers can find it difficult to trust digital banking services and may refrain from using digital banking services from a fear of frauds, data breaches or other kinds of harm.<sup>civ</sup> Without trust, customers may refrain from using digital services, limiting the benefits that could accrue from themselves and the BSP.

5

# CUSTOMER-CENTRIC PRIVACY PRINCIPLES FOR THE BANKING SECTOR



In this section, we identify a set of nine principles that offer actionable guidance to strengthen customer privacy and introduce data protection safeguards:

**Segregating personal data and ensuring visibility over personal data:**

BSPs must clearly catalogue and categorise the data they collect according to its sensitivity and the regulatory treatment the data must be afforded. BSPs must also maintain visibility over personal data throughout the data lifecycle.

---

**Communicating effectively with customers:**

Notices that BSPs provide to customers must be simple, comprehensible, and adequate. The notices should inform customers of how their personal data is collected, processed, stored, and shared, and the rights that customers have over their data.

---

**Obtaining informed consent from customers:**

BSPs must obtain consent from the customer before collecting personal data. The consent taken from customers must be informed, free, clear, specific, withdrawable and auditable.

---

**Collecting only accurate and proportionate personal data banking services:**

BSPs must collect and process only that personal data which is accurate and necessary for fulfilling the purposes that customers have consented to.

---

**Securing customers' personal data:**

BSPs must adopt strong technical, managerial, operational, and physical security safeguards to protect the confidentiality and integrity of personal data throughout the data lifecycle.

---

**Using or disclosing personal data with the consent of the customer for clear, specific and lawful purposes:**

BSPs must use personal data or disclose personal data to third parties only with the customer's consent and for pursuing a clear, specific and lawful purpose.





### **Enabling customers to access and rectify their personal data:**

BSPs must give customers access to their personal data and allow customers to rectify their personal data to ensure data accuracy.



### **Using automated means of processing responsibly:**

BSPs must complement the use of automated means of processing with adequate safeguards against risks, including strengthening human oversight over automated means.



### **Demonstrating compliance with best data protection practices:**

BSPs should be able to demonstrate their compliance with their stated data protection practices to the customers.



**PRINCIPLE 1****SEGREGATING PERSONAL DATA AND ENSURING VISIBILITY OVER PERSONAL DATA.**

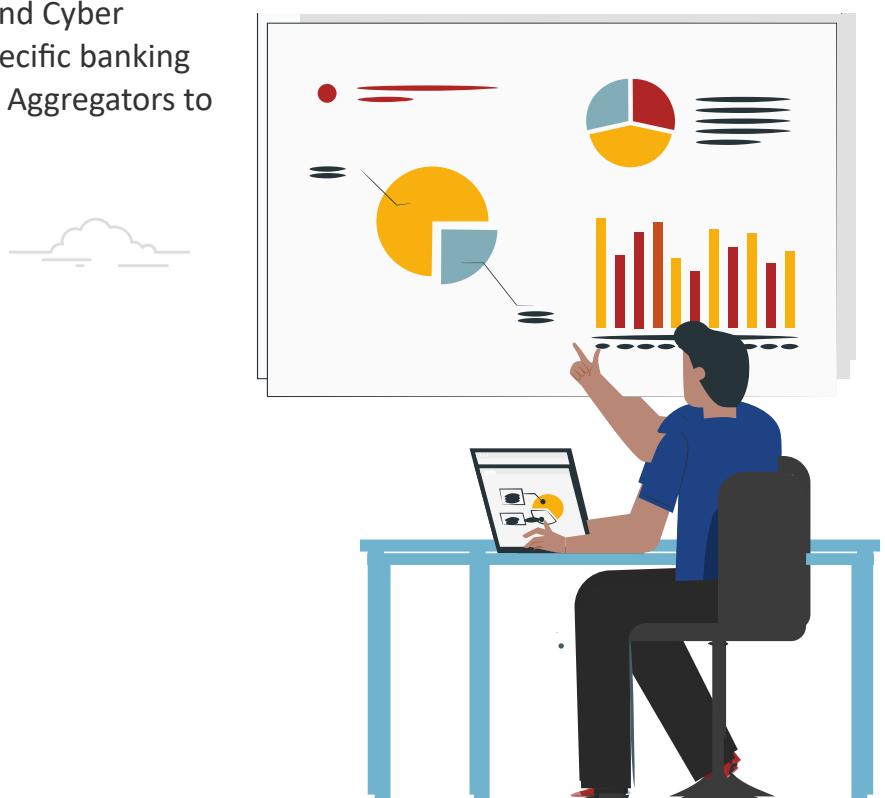
*BSPs must clearly catalogue and categorise the data they collect according to its sensitivity and the regulatory treatment the data must be afforded. BSPs must also maintain visibility over personal data throughout the data lifecycle.*

BSPs collect and process large amounts of data including personal and non-personal data which are often mixed. For example, a database in a bank may include both client information and transaction details for both individuals (personal data) and corporate entities (non-personal data).<sup>cv</sup> BSPs must be able to isolate personal data from this mix to understand the sensitivity of the data, what data protection and security measures they must employ, and what regulations they are subject to. This is the first and most important step for BSPs to protect personal data.<sup>cvi</sup>

In the same vein, BSPs must be able to identify personal data at different stages of the data lifecycle to ensure proper treatment. Unfortunately, BSPs may often find identifying and isolating personal data they process difficult. This can make personal data especially vulnerable when it is shared with third parties for processing. If it is impossible to isolate personal data from the mixed datasets then the mixed datasets should be treated as personal data.

BSPs must also have clearly defined processes for segregating, identifying, and creating inventories of the different kinds of data processes.

This principle is also found in key regulations applicable to BSPs,<sup>cvi</sup> such as the Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, 2016, which requires specific banking sector participants such as Web Aggregators to provide a notice (Ch. 2).



The key considerations for BSPs and measures BSPs can take for segregating data and mapping data flows are set out below:<sup>cviii</sup>



**i. Creating processes and standards for segregating personal data into different categories based on legal status or purpose of processing.** BSPs must –

- Develop policies for identifying and segregating different kinds of personal data.
- Segregate personal data directly collected from customers, and personal data collected indirectly.
- Segregate personal data to be processed for primary purposes and for secondary purposes.
- Create an inventory of processes and functions that involve personal information.
- Create an inventory of clients and partners with whom they share personal information.
- Map the personal data that is involved in each process, function or transaction.



**ii. Tracing personal data access and use trails to maintain visibility over personal data.** BSPs must–

- Map access to personal data by staff personnel and third parties.
- Identify third parties involved in its various processes, functions and transactions.
- Map the flow of personal data to third parties.
- Map technical assets that are involved in processing personal data.



**iii. Creating data custody policies about how personal data can be stored.** BSPs must–

- Define how personal data used for different processes, functions and transactions will be stored.
- Segregate data collected from customers, data captured through transactions, and data derived from processing personal data.
- Determine the level of protection and security different kinds of personal data should be given.
- Identify the personal data that can be pseudonymised or anonymised.



## CASE STUDY

### PRINCIPLE 1

# Segregating personal data and ensuring visibility over personal data.

AltaPine Ltd is a bank that has been serving its customers for more than 10 years. During that time, the bank acquired many customers. To serve the customers well, AltaPine entered into service agreements with many third parties.

One day, the banking regulator issued a notice to all the banks asking them to comply with its data protection and security direction. The direction also required AltaPine to submit a compliance report to the regulator on the security measures the bank undertook.

When AltaPine's management tried to comply with the direction, they realised that their data records were not segregated properly. They also did not keep a thorough record of data they shared with third parties. So, they did not know what measures they must take to secure different data records in their custody. As a result, the management was unable to comply with the regulator's direction. The regulator fined AltaPine for the lapse in data protection and security practices.

To avoid such situations BSPs should have a strict policy surrounding data segregation, data mapping and inventorying. This can help them understand their data protection and security obligations clearly. Otherwise, BSPs may adopt the wrong or inadequate safeguards to protect personal data.



**PRINCIPLE 2****COMMUNICATING EFFECTIVELY WITH CUSTOMERS.**

***Notices that BSPs provide to customers must be simple, comprehensible, and adequate. The notices should inform customers about the entity(ies) they are interacting with, how their personal data is collected, processed, stored, and shared, and the rights that customers have over their data.***

Providing easily accessible and comprehensible privacy notices about data processing activities is an important step in data protection. These notices serve two crucial objectives. First, the notices help BSPs gain the trust of customers, leading to greater uptake.<sup>cx</sup> Second, the notices help customers better understand how their personal data will be processed and what it implies for them, improving their autonomy.<sup>cxii</sup> This is especially important considering innovations in the banking sector like (i) Open banking where BSPs can share a customer's personal data with third-parties, and (ii) Disintermediated banking services that allow customers to bank through chat platforms and third party aggregators. In both cases, customers can find it difficult to understand the difference between the BSP and third parties, the provisions around data sharing in the BSP's privacy notice, and the implications of giving consent.<sup>cxii</sup>

Well-designed privacy notices can help customers overcome this challenge.

This principle is also found in key regulations applicable to BSPs,<sup>cxiii</sup> such as:



**Cross-sectoral regulations** such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires BSPs to provide a privacy notice to customers before collecting their personal data (Rule 4).

**Financial sector regulations** such as the Credit Information Companies Regulations, 2006 which requires BSPs to inform customers before collecting (or as soon as possible after collection) their credit information (Rule 11(3)).



**Banking sector regulations** like the Master Circular on Customer Service in Banks, 2015 (cl.25(1)), the Master Direction – Non-Banking Financial Company – Account Aggregator Directions, 2016 (cl.5), and the Master Circular – Credit card and debit card – Issuance and conduct directions, 2022 (cl.24), which require BSPs including Account Aggregators and card-issuers to provide a notice.

The key considerations for BSPs and measures they can take when providing notice to customers are set out below:



**i. Privacy notices must be designed in a user-centric manner so that customers can easily understand the provisions of the notice.**<sup>cxiv</sup>

- A privacy notice must not overwhelm or confuse customers by being too technical, specific, or broad.<sup>cxv</sup>
- Information presented in the notice must be plain, clear, concise, easily comprehensible, and adequately specific for customers to understand it properly.<sup>cxvi</sup>
- The notice must be made available in multiple languages when practicable.<sup>cxvii</sup>
- The notice must provide important information (like the purpose for processing personal data or details of redress mechanisms) prominently.<sup>cxviii</sup>
- Provisions that request consent from customers must also be placed distinctly from the general provisions in the notice.<sup>cxix</sup>
- BSPs should present a privacy notice to customers just in time for data collection.<sup>cxx</sup>



**ii. Privacy notices, including those presented by Account Aggregators, must inform customers about the important aspects of personal data processing activities.**<sup>cxxi</sup>

- a. A privacy notice should clearly disclose:<sup>cxxii</sup>
  - The types of personal data that will be collected, both, directly from the customer and indirectly from third parties;
  - The types of data that are mandatory and optional for a processing activity;
  - The purposes for which BSPs will process personal data, which must be clear, specific and lawful;
  - The duration for which BSPs will retain personal data;
  - The personnel and entities would be able to access the data;
- b. The notice should also provide details about customers' rights over their data, grievance redress mechanisms and ways to report misuse or breach of data.



**iii. BSPs should ensure that customers are aware when they are interacting with third parties** including chat platforms, third party apps and account aggregators.

**iv. Privacy notices must clearly inform customers about the use of automated means.**

The privacy notice must inform customers—<sup>cxixiii</sup>

- That their personal data may be processed by automated means;
- That they may interact with automated systems, and
- About mechanisms through which they can contest or seek explanation of decisions reached through automated means.





## CASE STUDY

### PRINCIPLE 2

# Communicating effectively with customers.

Pranav wants to take a loan for purchasing an air conditioner. He uses BarFinance, a digital banking marketplace, to look for loan. Pranav finds F11 Bank's loan product most attractive. When he selects the product, a lengthy notice appears for him notifying him about receiving a consent request from DTE AA, and to accept or decline. Alarmed by the length of the form, Pranav skips reading the form. Instinctively, he chooses the 'Accept' option.

Sometime later, Pranav receives a mail from 'DTE AA' asking for his consent to share sensitive financial information with F11 Bank. Being unsure about what DTE AA is and why it wants Pranav's information, Pranav declines DTE AA's request. Soon after, Pranav receives a notification from F11 bank saying his loan application is rejected. Upon inquiry, Pranav understands that DTE AA is an account aggregator, and that DTE AA would help transfer important information for processing Pranav's loan application.

Providing lengthy notices can dissuade customers from reading them fully. As a result, they may be unaware of important steps in their journey with the BSP. This can hamper their experiences with the BSP, as seen in Pranav's case.

To avoid such situations BSPs should provide clear and easily comprehensible notices to customers. These notices should help customers easily understand their rights and obligations when using a service, including in relation to their personal data. The notice should clearly notify customers about any third parties they may interact with and for what purpose. Doing so can help customers feel more informed and comfortable with the process.





**PRINCIPLE 3****OBTAINING INFORMED CONSENT FROM CUSTOMERS.**

***BSPs must obtain consent from the customer before collecting personal data. The consent taken from customers must be informed, free, clear, specific, and withdrawable.***

Consent is a crucial part of data protection which enables customers to exercise choice and control over how their personal data is used.<sup>cxxiv</sup> Account Aggregators can play a big role in making consent artefacts more accessible and intuitive for different customer segments. Basing processing activities on customers' consent can help BSPs reduce customers' apprehensions about risks and build trust.<sup>cxxv</sup>

This principle is also found in the following key regulations applicable to BSPs:<sup>cxxvi</sup>



**Cross-sectoral regulations** such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) (Rule 5 and rule 6) and the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (s.29-30) which require BSPs and UIDAI to obtain customers' consent for processing personal data or sharing it with third parties.

**Banking sector regulations** such as the Master Direction – Know Your Customer (KYC) Directions, 2016 (cl.3(xx), cl.13, cl.17(1), cl.56), the Master Circular on Customer Service in Banks, 2015 (cl.25(1)) and Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions (cl.5-8) require BSPs including Account Aggregators to take customers' consent before collecting, and processing personal data.

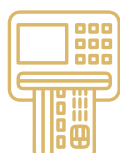


The key considerations for BSPs and measures they can take when obtaining consent from customers are set out below:



**i. By law, consent must be informed, free, clear, specific, withdrawable and auditable.**<sup>cxxvii</sup>

- Customers must have all relevant information to give an informed consent.
- Customers should give consent freely and voluntarily without being forced or misled.
- Customers must give consent clearly and expressly.
- Customers must be able to give consent separately for the different purposes of processing personal data.
- Customers should be able to withdraw their consent. Withdrawing consent must be as easy as giving consent.
- Customers should be able to audit all data sharing transactions performed by a BSP.
- BSPs must be able to demonstrate that the consent they obtained from customers satisfies the elements above.



**ii. Customers should not face barriers for giving or withdrawing consent.**

- BSPs should allow customers to manage their consent preferences through entities such as consent managers.<sup>cxxviii</sup>
- Customers should be able to use the same channels for giving and withdrawing their consent.
- To be accessible to less digitally savvy, less literate, or differently abled customers, the processes should:
  - a. Guide customers in understanding privacy notices and consent;
  - b. Provide alternate means of seeking and recording consent for differently abled customers, and
  - c. Help customers provide consent through visual and aural channels.



**iii. BSPs must design consent processes that strengthen customers' privacy.**<sup>cxxix</sup>

- BSPs should disclose risks that could arise for customers from giving consent and the measures that BSPs have taken to mitigate those risks.<sup>cxxx</sup>
- BSPs should disclose the use of automated systems for providing products and services to customers.<sup>cxxxi</sup>
- BSPs should not assume customers' consent by default. BSPs must take fresh consent from customers when they collect new personal data or begin new processing activities.<sup>cxxxii</sup>
- They must allow customers to opt-in and give express consent to processing activities.<sup>cxxxiii</sup>
- Customers must be able to refuse consent for optional processing activities without facing any detriment to the services they receive.<sup>cxxxiv</sup>
- Customers should be able to withdraw their consent and opt-out of processing activities without detriment other than termination of services.<sup>cxxxv</sup>
- BSPs should maintain records of customers' consent preferences, consent withdrawals and correspondence with the customers when obtaining consent.<sup>cxxxvi</sup>





## CASE STUDY

### PRINCIPLE 3

# Obtaining informed consent from customers.

Sarah had previously purchased a credit card from a BSP. At the time of purchase, she had consented to the BSP's use of her personal data according to the privacy notice that was given to her.

However, Sarah was recently made aware of changes to the privacy notice without her consent. Sarah was not informed in advance about changes to the privacy notice. The BSP did not take her consent for processing her personal data under the new privacy notice.

Sarah does not want to consent to the changes and chooses to withdraw her consent. On approaching her BSP, Sarah learns that the process for withdrawing consent is long-winded, involving complex procedures. The BSP had not informed Sarah about these complex procedures for withdrawing consent when she purchased the credit card.

These practices preclude Sarah from giving free, clear, and informed consent and make it challenging for Sarah to withdraw her consent. In many jurisdictions, a unilateral change in consent policies would render the initial consent null and void.

To avoid this, BSPs must build consent artefacts that are accessible to customers facing a variety of barriers, including physical and mental disabilities. Further, the consent artefacts must allow customers to withdraw consent with the same ease as giving consent and must be presented in a manner that customers can easily understand how to manage consent. BSPs must keep track of customers' consent preferences to understand the terms and conditions for which they have customers' consent, and those for which they must take consent afresh.

Account Aggregators may be able to play a vital role in these cases by not only simplifying consent management through various means, such as by creating consent dashboards and intuitive consent artefacts to suit customers.



**PRINCIPLE 4****COLLECTING ACCURATE AND PROPORTIONATE PERSONAL DATA FOR PROVIDING BANKING SERVICES.**

*BSPs must collect and process only that personal data which is accurate and necessary for fulfilling the purposes that customers have consented to.*

The personal data that BSPs process must satisfy two important criteria. First, BSPs must process only that personal data that is necessary for fulfilling the purposes that customers consented to. Processing unnecessary personal data could be intrusive and violates customers' privacy.<sup>xxxxvii</sup> Second, the personal data processed must be accurate. Processing inaccurate personal data can lead to inaccurate decisions, sub-optimal products and services, and poor financial outcomes for the customers.<sup>xxxxviii</sup> BSPs can rely on the Account Aggregator framework to collect accurate and updated information about customers. However, BSPs should ensure that they only query information that is necessary and use that information only for purposes customers consented to.

This principle is also found in key regulations applicable to BSPs,<sup>xxxxix</sup> such as:



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**SPDI Rules**) (Rule 4 and rule 5) and the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (s.31) which requires BSPs and UIAs to collect and process only necessary and accurate personal data.

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which requires BSPs to take measures to ensure credit information they process is accurate, complete, and necessary for the purposes of processing (Chapter VI).



**Banking sector regulations** like the Master Direction – Know Your Customer (KYC) Directions, 2016 (cl.38) which require banks to ensure data quality.

The key considerations for BSPs and measures BSPs can take for ensuring data quality are set out below:



**i. The personal data collected and processed by BSPs must be proportionate and accurate.**

- Personal data processed by BSPs must be relevant and necessary for fulfilling the purpose of processing personal data.
- BSPs must delete personal data that is not necessary for processing.
- Personal data should be accurate, complete, representative, unbiased, up-to-date and not misleading.
- The collection of data to meet this quality should be consensual, lawful, fair, and non-intrusive.
- BSPs should collect new personal data only if it is necessary for maintaining accuracy or fulfilling a purpose.<sup>cxli</sup>
- BSPs should undertake data protection impact assessments to ensure they are only processing proportionate personal data.



**ii. BSPs must have mechanisms to verify the quality of the personal data they process. BSPs must:**

- Frequently assess if the personal data being processed is inaccurate or out-of-date.<sup>cxli</sup>
- Assess the quality and relevance of personal data for the purposes it is being processed.<sup>cxlii</sup>
- Institute mechanisms to filter out incomplete, inaccurate, or unnecessary personal data during data collection.<sup>cxliii</sup>
- Assess alterations in personal data from breach or cyberattack to rectify inaccuracies.<sup>cxliv</sup>
- Regularly review outputs from processing that are used as feedback or inputs for automated means of processing.<sup>cxlv</sup>
- Review processing activities to identify and rectify causes of bad data quality.<sup>cxlvi</sup>
- Create protocols for assessing the quality of data collected from third parties.<sup>cxlvii</sup>
- Maintain records of the source from where personal data was collected.<sup>cxlviii</sup>
- Maintain records of the measures taken to check the accuracy of data.<sup>cxlix</sup>
- Maintain records of inaccuracies and challenges to the accuracy of personal data arising from customers' access rights.<sup>cl</sup>



## CASE STUDY

### PRINCIPLE 4

# Collecting accurate and proportionate personal data for providing banking services.

Khyaati has been a customer of GloBank, a commercial bank, for the past ten years. Most of her financial transactions took place through GloBank. Khyaati recently married Mathew. They wanted to open a joint account together to make transactions easily. Mathew, being an existing customer of CBH Bank, proposes to open a joint account in that bank. CBH Bank asks Khyaati for her KYC information to open the account, upon that Khyaati decides to share her CKYC information.

Khyaati received a data transfer request from an Account Aggregator on behalf of CBH bank. She noticed CBH bank had requested her financial transaction history. Khyaati declined consent for accessing her financial transactions because she did not find it relevant for opening a joint bank account. CBH bank insisted on Khyaati's transaction history. Khyaati felt that the BSP did not respect her privacy and interests. She and Mathew decided to open a joint account in another bank.

To avoid such situations, BSPs must collect and process accurate personal data which is necessary for fulfilling a purpose that customers consent to. BSPs should establish mechanisms that can help examine the accuracy and proportionality of personal data before and during the processing of personal data. BSPs can rely on different measures, like performing Data Protection Impact Assessments (**DPIAs**), to understand which data is necessary. BSPs can also regularly review the need to continue processing personal data. Further, they must allow customers access to the personal data they are processing and adhere to customer's choice of revoking consent for processing that data.





**PRINCIPLE 5****SECURING CUSTOMERS' PERSONAL DATA.**

***BSPs must adopt strong technical, managerial, operational, and physical security safeguards to protect the confidentiality and integrity of personal data throughout the data lifecycle.***

Customers' privacy and integrity of personal data are vulnerable to cyberattacks, fraud and data breaches that can expose customers' money to malicious actors.<sup>cli</sup> These risks may grow larger as banking services become more digital, or fully digital as in the case of neo-banks.<sup>clii</sup> BSPs should take a variety of technical, managerial, operational and physical security measures that can protect the confidentiality and integrity of personal data throughout the data lifecycle.<sup>cliii</sup> These measures must supplement other data protection practices like providing a privacy notice and obtaining consent. BSPs risk the reputation and integrity of processing activities in the absence of proper security safeguards.<sup>cliv</sup>

This principle is also found in key regulations applicable to BSPs,<sup>clv</sup> such as:



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires BSPs to adopt security safeguards that can adequately protect the personal data that they process or share with third parties (Rules 8 and 9).

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which require BSPs to take measures to put proper security safeguards into place to protect credit information (Section 19, section 20, and section 22).



**Banking sector regulations** like the Mobile Banking transactions in India – Operative Guidelines for Banks, 2016 (cl. 8 and Ann. II), Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, 2006 (cl.5.6 and 5.9), the Guidelines on Information Security, Electronic Banking, Technology Risks Management and Cyber Frauds, 2016 (Ch,1-9), Cyber Security framework in Banks, 2016 (Ann.I-III), and the Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016 (cl.7, 8 and 14), which require BSPs to adopt a variety of data security safeguards.



The key considerations for BSPs and measures BSPs can take for ensuring robust data security safeguards are set out below:<sup>clvi</sup>



**i. BSPs must identify the vulnerabilities and risks that must be addressed through security safeguards. BSPs must:**

- Conduct risk assessments, threat tests and information audits to understand vulnerabilities and risks to personal data.<sup>clviii</sup>
- Conduct data protection impact assessments and threat analyses before using new technologies to process personal data.<sup>clix</sup>
- Gauge the risk of reidentification for anonymised data through continuous review.<sup>clx</sup>



**ii. BSPs must establish security safeguards that are proportionate to the risks identified. BSPs must:**

- Identify data protection guarantees in the privacy notice that must be operationalised through security safeguards.<sup>clxi</sup>
- Adopt technological measures including encryption and use of passwords.<sup>clxii</sup>
- Adopt organisational measures including oversight and control mechanisms, accountability, periodic evaluation, defining data access, data authentication and authorisation protocols.<sup>clxiii</sup>
- Adopt physical measures including security clearances to personal data servers.<sup>clxiv</sup>
- Deploy a data breach and incident management process that can—<sup>clxv</sup>
  - a. help in addressing existing vulnerabilities and threats to personal data, and
  - b. help customers take steps to mitigate risks to personal data.
- Ensure personal data that is not relevant for processing is deleted or blocked when sharing with third parties;<sup>clxvi</sup>
- Ensure personal data is deleted carefully without giving access to unauthorised parties.<sup>clxvii</sup>
- Implement anonymisation and deidentification techniques.<sup>clxviii</sup>
- Periodically rectify automated means of processing based on audits and assessments.<sup>clxix</sup>
- Create controls to recover accidentally lost, altered, or destroyed personal data.<sup>clxx</sup>
- Regularly review security safeguards through audits, assessments, and threat tests to identify and eliminate vulnerabilities.<sup>clxxi</sup>

- Implement and operationalise privacy-by-design principles<sup>i</sup> and security-by-design principles<sup>ii</sup> throughout the data lifecycle.
- Share intelligence on threats with other BSPs to strengthen the banking ecosystem.<sup>clxxii</sup>
- Create awareness among customers about good security practices they should follow.<sup>clxxiii</sup>



**iii. BSPs must ensure security safeguards in sharing personal data with third parties.** BSPs must—

- Map all the entities with which they have interconnections and interdependencies.<sup>clxxiv</sup>
- Assess the risks that could arise from outsourcing personal data to third parties.<sup>cxxv</sup>
- Create controls to ensure third parties use personal data only to fulfil the purposes mentioned in their outsourcing agreement.<sup>cxxvi</sup>
- Supervise and ensure that the third parties have adequate security safeguards to protect personal data.<sup>cxxvii</sup>
- Introduce breach notification requirements in outsourcing agreements with third parties.
- Incorporate measures to monitor personal data flows through Application Programming Interfaces (APIs) with third parties.
- Auditing third parties using APIs for data malpractices.



**iv. AAs must incorporate strong technical safeguards that can help operationalise data protection principles.** BSPs must—<sup>clxxviii</sup>

- Incorporate end-to-end encryption of data transfers.
- Implement authentication capabilities to verify partners and customers' identities.
- Regularly monitor the cyber landscape for threats.
- Upgrade technical infrastructure and stop relying on poor infrastructure.



**v. API providers must ensure risk-proportionate security safeguards.**

API providers must —

- **Incorporate strong authentication and authorisation controls into the APIs** to ensure the integrity of personal data flow.



## CASE STUDY

### PRINCIPLE 5

# Securing customers' personal data.

“BancAll” is a leading digital banking marketplace application in India. It is a pioneer in using technology to support its services. Apart from collecting data from the customer, BancAll collects data indirectly from multiple sources like the retail partners on its platform. BancAll stores this data in a centralised database. It uses APIs to share information with authorised third parties for enhancing customer experience and for improving business opportunities.

BancAll suffered a data breach that leaked highly sensitive customer information including KYC information, payment transaction details, contact details and product purchase history. An independent investigation found that BancAll did not take measures to secure data that was shared with third parties. The APIs that BancAll used did not have strong security features that could protect personal data shared through them. Further, BancAll did not take proper measures to ensure that third parties with which it shared information had strong security safeguards. Hackers were able to exploit these vulnerabilities to access customers' data.

BancAll was negligent in implementing technical and procedural controls to ensure security of customer data throughout the data lifecycle. BancAll made itself vulnerable due to improper oversight over its data-sharing practices and relevant security safeguards. BancAll should have tested the APIs' security before using them and take measures to address any vulnerabilities. It should have also incorporated strong oversight, access and authorisation controls to better plug gaps in APIs. Similarly, BancAll should have examined its third-party partners' security practices for vulnerabilities that must be addressed through appropriate controls.



**PRINCIPLE 6****USING OR DISCLOSING PERSONAL DATA WITH THE CONSENT OF THE CUSTOMER FOR CLEAR, SPECIFIC AND LAWFUL PURPOSE.**

***BSPs must use personal data or disclose personal data to third parties only with the customers' consent and for pursuing a clear, specific and lawful purpose.***

BSPs may have primary purposes (like the provision of banking services), and secondary purposes (like cross-selling services or fulfilling legal and regulatory obligations) for using or disclosing personal data to third parties. Both primary and secondary purposes must be clear, specific and lawful.

Further, in both cases, the BSPs must inform such use or disclosure to customers as part of their notice and take consent from customers before processing personal data. These measures can make processing activities more transparent and predictable for customers.<sup>clxxxix</sup>

Further, customers should be able to request BSPs to disclose their personal data to other entities through data portability. Data portability allows customers to request BSPs to have their personal data transferred to any other entity in a machine-readable format. This can help operationalise customers' autonomy over whom their personal data is shared with.<sup>clxxx</sup>

This principle is also found in key regulations applicable to BSPs,<sup>clxxxi</sup> such as:



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires BSPs to process personal data and disclose personal data for specific purposes and with customers' consent (Rules 5 and 6).

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which requires BSPs to adopt principles determining what purposes credit information can be used for and when it can be disclosed (Section 20) or the Aadhaar Act, which requires BSPs to obtain consent from an individual before collecting their identity information for the purposes of authentication (section 8).



**Banking sector regulations** like the Reserve Bank of India (Credit Card and Debit Card – Issuance and Conduct) Directions, 2022, which requires BSPs to obtain explicit consent from an individual before disclosing any information obtained from them at the time of opening their account or issuing a card to them (clause 27).<sup>clxxxii</sup>

The key considerations for BSPs and measures BSPs can take to ensure appropriate data use and disclosure are set out below:



- i. BSPs should process personal data only for the purposes customers consented to.** BSPs processing personal data for other purposes must be able to demonstrate a direct connection to the stated purpose.<sup>clxxxiii</sup>



- ii. BSPs should use or disclose personal data for clear, specific and lawful purposes that customers consented to.** BSPs must—<sup>cxxxiv</sup>

- Maintain a specific list of third parties to whom personal data may be disclosed.
- Disclose a list of purposes for which personal data may be disclosed to third parties.
- Stop disclosing personal data to third parties if customers withdraw consent.
- Facilitate communication between customers and third parties where necessary.<sup>clxxxv</sup>
- Ensure that they only share data that is accurate and necessary.<sup>clxxxvi</sup>



- iii. BSPs must operationalise data portability for customers on their request.** BSPs must—<sup>cxxxvii</sup>

- Install mechanisms to receive and record data porting requests from customers.
- Adopt organisational policies and capacity to recognise and operationalise data porting requests.
- Verify the identity of the customer requesting for porting before transmitting data.
- Respond to porting requests in a timely manner.
- Receive and transmit personal data to third parties on customers' request.
- Transmit personal data on customers' request without placing financial, legal or technical obstacles.
- Transmit data on customers' request in a structured, commonly used and machine-readable format.
- Transmit data on customers' request in a secure method.



**iv. APIs used for transferring personal data should be secure and prevent leakages. BSPs must –**

- Incorporate authentication and authorisation controls to ensure integrity of personal data flow.
- Ensure the APIs are secure against technical breaches or inadvertent data leakages due to broad queries.<sup>clxxxvii</sup>



**v. BSPs may use AAs to simplify consent management for customers.**

The AAs should – <sup>cxxxix</sup>

- Clearly convey key information that is necessary for customers to form informed consent.
- Ensure they collect and use personal data only when it is necessary.
- Be accessible and comprehensible for a diverse set of customers.
- Be intuitive and designed to suit customers' attitudes, needs, behaviours and expectations.
- Take consent for specific purposes without assuming broad consent from the customer.
- Be secure and operationalise key data protection safeguards.
- Allow customers to dispute instances of unauthorised retrieval or access to personal data.



**vi. BSPs should maintain their assessments of customers distinctly from customers' personal data to aid data portability.<sup>cxc</sup>**



## CASE STUDY

### PRINCIPLE 6

# Using or disclosing personal data with the consent of the customer.

Sameera, a chemist, wanted to obtain a credit card that offers gift vouchers for her preferred electronic commerce website. She approached a BSP who could meet her requirements. As part of the onboarding process, the BSP asked Sameera to share some personal information including her identification documents, contact details and her type of employment, including the fact that she works as a chemist. Sameera read the terms and conditions about how the BSP uses personal information carefully and decided to share her information believing that it would be used only for the operation of the credit card.

A few days after sharing information, Sameera began receiving messages from multiple online pharmacies about special tie-ups with chemist. Alarmed by the messages, Sameera contacted some of the online pharmacies to find out how they got her contact details. She found that her BSP had shared her personal information with the online pharmacies. Sameera read the BSP's privacy policy and her banking agreement again to verify if she gave her consent to the BSP for sharing her personal information with online pharmacies. Neither document mentioned with whom the BSP can share Sameera's data and for what purpose. The BSP disclosed Sameera's information to the online pharmacies without her consent. Sameera was compelled to give blanket consent and allow the BSP to share her data for secondary purposes that she did not prefer.

The BSP must stop disclosing Sameera's information to online pharmacies and with any other third party they may be disclosing information to. The BSP must clearly inform Sameera with whom they will share personal information and for what specific purpose. The BSP should allow Sameera to consent separately for primary and secondary purposes. Sameera must be able to choose how her personal data is used and who it is shared with. Further, the BSP should not deny Sameera banking services, the primary purpose for which personal data was processed, because she denied consent for secondary purposes of processing personal data.





**PRINCIPLE 7****ENABLING CUSTOMERS TO ACCESS AND RECTIFY THEIR PERSONAL DATA.**

*BSPs must give customers access to their personal data and allow customers to rectify their personal data to ensure data accuracy.*

Providing customers access to their personal data is an important part of upholding their autonomy<sup>cxci</sup> and maintaining data quality. Having access to information about processing activities can help customers stay informed and make decisions about how their personal data is used. In the same vein, customers will be able to identify inaccuracies in a BSPs' personal data records and rectify them. This would ensure BSPs process accurate data about customers.<sup>cxcii</sup>

This principle is also found in key regulations applicable to BSPs,<sup>cxci</sup> such as:



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires BSPs to enable access and rectification of personal data records by customers (Rule 5).

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which requires BSPs to enable access and rectification of personal data records by customers (Section 20(a)(iii)).





The key considerations for BSPs and measures BSPs can take for enabling customers to access and rectify their personal data are set out below:



**i. BSPs must establish processes for enabling access and rectification.**

BSPs should – <sup>CXCIV</sup>

- Clearly communicate access and rectification processes to customers.
- Facilitate customer's right to access personal data in a structured, machine-readable format.
- Enable access and rectification for personal data collected directly from the customer and indirectly from third parties.<sup>CXCV</sup>
- Facilitate customer's ability to access and rectify their personal data when they choose without cost or delay.
- Allow customers to modify their personal data through diverse channels, including physical channels and digital portals.<sup>CXCVI</sup>
- Make changes to personal data records to match the modifications made by customers.<sup>CXCVII</sup>



**ii. BSPs should notify third parties about changes in personal data.**

BSPs must- <sup>CXCVIII</sup>

- Provide third parties with amended personal data records when necessary.<sup>CXCIX</sup>
- Take measures to ensure third parties rectify their personal data records.<sup>CC</sup>



**iii. BSPs must provide customers information about important processing activities. BSPs must –<sup>CCI</sup>**

- Give customers information about important processing activities, including processing through automated means.<sup>CCII</sup>
- Meaningfully communicate the implications, intended effects and rationale involved in automated means of processing.<sup>CCIII</sup>
- Demonstrate through prior assessments that automated tools provide legitimate outputs without discrimination.<sup>CCIV</sup>
- Provide customers with a standard list of third parties to whom personal data may be disclosed.<sup>CCV</sup>

**CASE STUDY****PRINCIPLE 7**

## Enabling customers to access and rectify their personal data.

Rahul applied through an online app for a Buy-Now-Pay-Later (BNPL) card to avail of cashback offers. The online app quoted a very high fee and interest rate citing his low credit score. Rahul could not understand why his credit score was low as he did not have any outstanding debt, had never applied for a loan before and only had one credit card issued by his BSP on which he had never made a late payment.

Rahul contacted his BSP's branch to inquire about his low credit score. After speaking with his relationship manager, he realized that his credit score had fallen because his credit card transaction history showed an incorrect large outstanding payment for a transaction he had never made. He asked his relationship manager on the procedure for rectifying the error. He was informed that he must register himself on the BSP's web portal to raise a dispute and seek a resolution. After doing so, he did not receive any response or resolution.

Rahul wrote a formal request to the BSP along with relevant documentation to rectify the incorrect outstanding payment. However, he did not receive a response from the BSP. As a result, Rahul was unable to apply for the BNPL card.

To avoid this, BSPs must provide customers with a variety of channels to access and rectify their personal data records. BSPs must also develop standard procedures to rectify personal data records and communicate rectifications to third parties promptly.

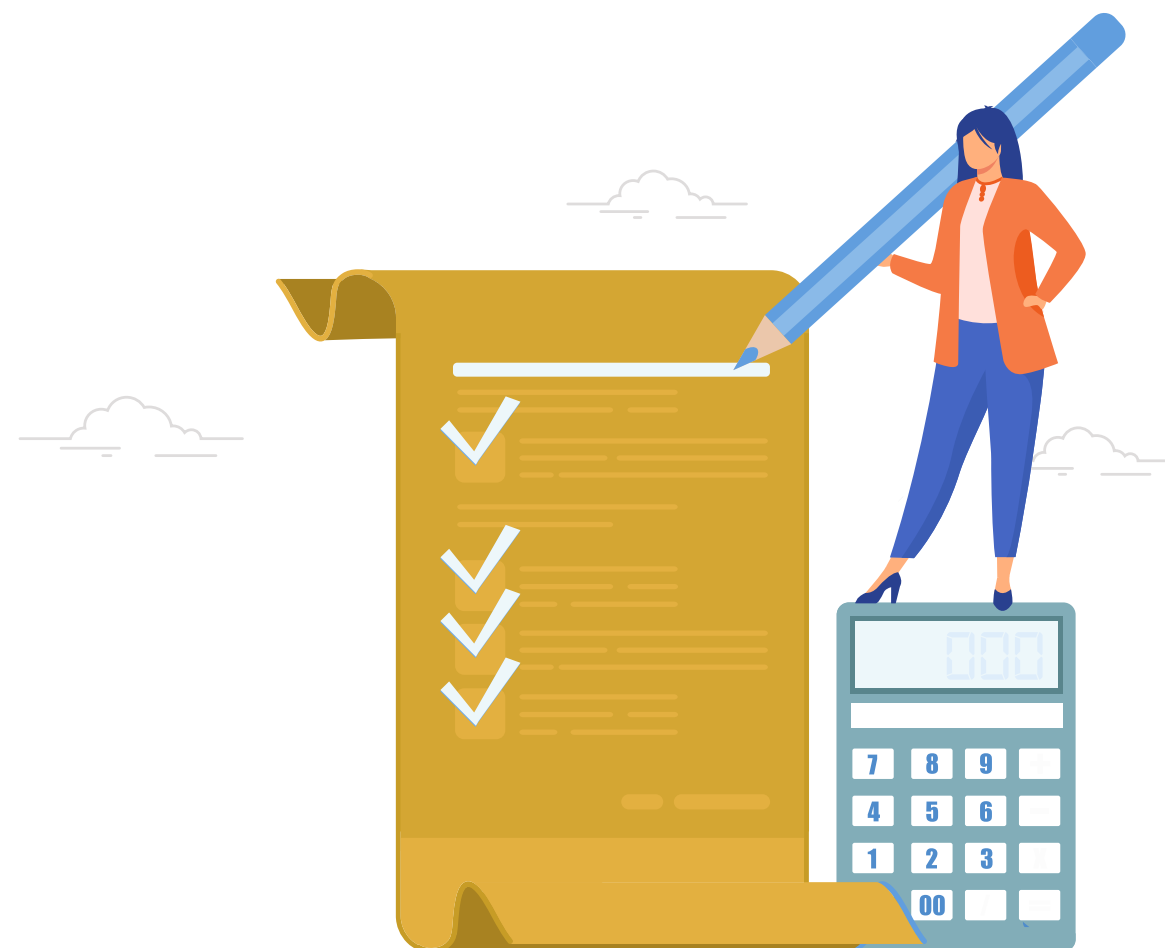


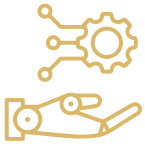
**PRINCIPLE 8****USING AUTOMATED MEANS OF PROCESSING RESPONSIBLY.**

***BSPs must complement the use of automated means of processing with adequate safeguards against risks, including, strengthening human oversight over automated means.***

BSPs may use automated means for different purposes like assessing the risk profile of a customer. Outputs produced by automated means could pose unintended risks for BSPs and customers without adequate safeguards. The risks for BSPs could include adverse selection and poor risk assessment of customers. The risks for customers could include unjust rejections, unsuitable products, and risks to privacy. Further, BSPs may be unable to understand or explain why automated means produced a certain output. BSPs should adopt and use automated means responsibly to avoid risk and protect customers' interests. These concerns have been recognised by the RBI in recent years. In the Digital Lending Report, a key immediate recommendation is that regulated entities will have to document *"the rationale for the algorithmic features aiding lending decisions that should ensure necessary transparency"*.

To be in compliance with leading regulatory frameworks, BSPs can draw upon global best practices developed by practitioners and multilateral organisations. The key considerations for BSPs and measures BSPs can take for using automated means responsibly are set out below:





**i. BSPs must strengthen human oversight over automated means.** BSPs must—<sup>ccviii</sup>

- Install measures to ensure transparency, auditability, accountability and explainability of decisions made by automated means.
- Explain the decision-making process of the automated means in clear, comprehensible and accessible terms.
- Record actions taken to identify, document and mitigate risks to customers' rights from automated means.
- Document the datasets and processes that are used by automated means to arrive at decisions.
- Implement effective management and oversight controls over third-party vendors providing automated means.<sup>ccix</sup>



**ii. BSPs must adopt safeguards against risks posed by automated means of processing.** BSPs must—<sup>ccx</sup>

- Preemptively identify risks to the safety and rights of customers from using automated means of processing by sandboxing or piloting.
- Ensure that the automated means are fit for purpose of processing by clearly understanding the purpose for which they were developed, their capabilities and limitations.
- Test the robustness, reliability, accuracy, and security of automated means before putting them into use.
- Ensure that the data which is being processed is representative, unbiased and of high-quality.
- Debias personal data processed by automated means where necessary.
- Adopt best standards for gathering and labelling personal data that will be used for processing by automated means.
- Identify and address any bias in the decision-making process by automated means.
- Continually identify vulnerabilities in the automated means used for processing.
- Conduct periodic reviews and monitor automated means.<sup>ccxi</sup>
- Develop measures to mitigate the risks identified from automated means of processing.
- Upskill personnel who develop and administrate automated means of processing to ensure responsible processing.



**iii. BSPs must give customers control over decisions made through automated means. BSPs must–**

- Notify customers through all service delivery channels that automated means may be used for making decisions about the customer.<sup>ccxii</sup>
- Allow customers to contest decisions made through automated means.<sup>ccxiii</sup>
- Create transparent processes for customers to submit complaints about decisions made through automated means.<sup>ccxiv</sup>
- Create a variety of channels for customers to contest or seek review of decisions made through automated means.<sup>ccxv</sup>
- Create clear processes for customers to seek redress when their rights are harmed by processing by automated means.<sup>ccxvi</sup>
- Provide data management tools that can help customers review, edit, and update personal data that is processed through automated means.<sup>ccxvii</sup>
- Make customers aware of their rights in relation to how their personal data is processed through automated means.<sup>ccxviii</sup>





## CASE STUDY

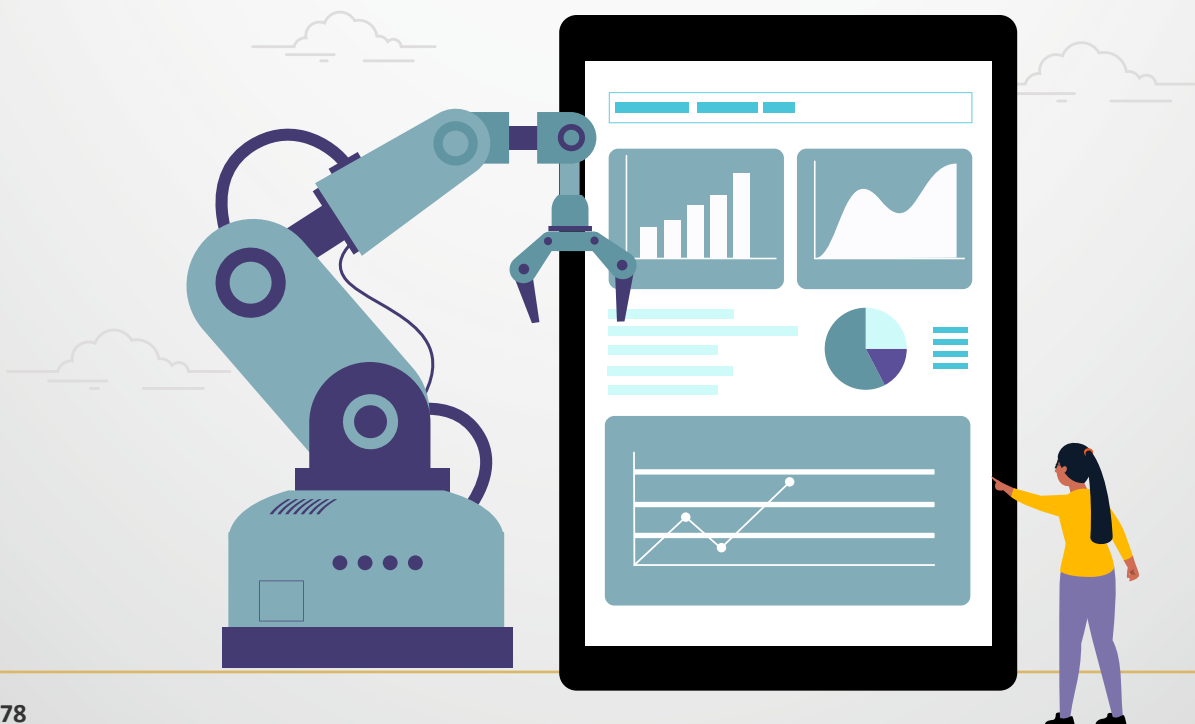
### PRINCIPLE 8

# Using automated means of processing responsibly.

Anuj and Harshitha both applied for loans from the same BSP. Both their credit scores and loan requirements are the same and they applied for a loan for the same amount under the same scheme. However, the BSP rejected only a fraction of Harshitha's application while accepting Anuj's application.

On raising the issue with the BSP, the BSP explained that the processing of loan applications is automated and based on credit models that use complex algorithms secured from a vendor. The BSP is unable to explain why Harshitha's application was rejected even when Anuj's application was accepted in its entirety.

BSPs using automated means of processing must install strong controls, oversight mechanisms and customer safeguards. BSPs must be able to trace the decision-making process of an automated system and explain the decision in simple terms to customers. BSPs must also preemptively identify risks from using automated means, like discrimination between customers, and take adequate measures to mitigate those risks.



**PRINCIPLE 9****DEMONSTRATING COMPLIANCE WITH BEST DATA PROTECTION PRACTICES.**

*BSPs should be able to demonstrate their compliance with their stated data protection practices to the customers.*

BSPs must be able to demonstrate their compliance with data protection practices.<sup>ccxix</sup> BSPs could adopt a variety of transparency and accountability measures to do so. Transparency and accountability play crucial roles in developing a relationship of trust with customers. Through transparency and accountability, BSPs can demonstrate and reassure customers that their personal data is being used safely and responsibly in a way that safeguards privacy.

The principle has been embedded into the existing data protection regime in India across different regulations. These regulations mostly aim to facilitate and ensure regulatory compliance. However, BSPs could leverage the same obligations to build trust with customers. Some key regulations are set out below.<sup>ccxx</sup>



**Cross-sectoral regulations** like the Information Technology Act, 2005 which requires providers intermediating information flows to maintain records of activities specified by the Central Government (s.67C). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 also require BSPs to be able to demonstrate that they follow the best practices for data protection (Rule 8).

**Banking sector regulations** like the Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, which require Account Aggregators to establish a Citizen's Charter that explicitly guarantees protection of the rights of a customer and a risk management framework that includes deploying strong authentication to protect access to customer data and systems.



The key considerations for BSPs, and the measures that can be taken by BSPs for ensuring accountability in processing activities are set out below: <sup>ccxi</sup>



**i. BSPs should create organisational capacity for personal data protection.**

BSPs should: — <sup>ccxxii</sup>

- Ensure senior management is conscious about protecting customers' personal data.
- Train their staff and personnel to answer inquiries about the BSP's privacy policies, consent processes, security safeguards and redress processes.
- Inform third-party service providers about past vulnerabilities and attacks.



**ii. BSPs should create technical capacity to ensure data protection.**

BSPs must-

- Improve technical systems and capacity by moving away from paper-based and legacy systems.
- Constantly review and upgrade data protection and security measures.



**iii. BSPs should demonstrate their compliance with data protection laws and best practices.** BSPs should: <sup>ccxxiii</sup>

- Adopt board-approved policies committing to protect personal data by default.
- Create oversight mechanisms at the senior management-level to ensure compliance with data protection policies.
- Appoint personnel who would monitor the BSPs' compliance with data protection law and ensure best practices in data protection.
- Publish the names of personnel responsible for ensuring the BSP follows robust data protection practices.
- Conduct audits to assess effectiveness of privacy notices, security safeguards and key data protection practices.
- Maintain records of different aspects of processing activities including—
  - a. source from where personal data was collected;<sup>ccxxiv</sup>
  - b. measures taken to check accuracy of data;<sup>ccxxv</sup>
  - c. processing activities that were undertaken with the personal data;
  - d. disclosure of personal data to third parties;
  - e. security safeguards installed, and<sup>ccxxvi</sup>
  - f. data protection impact assessments conducted prior to processing personal data.



- Develop, document and implement data policies defining—<sup>ccxxvii</sup>
  - a. protocols for implementing a privacy by design policy;
  - b. protocols for collection, access and use;
  - c. protocols for retaining and deleting personal data;
  - d. means to ensure data quality;
  - e. security safeguards and risk assessment frameworks;
  - f. protocols for implementing a security by design policy;
  - g. protocols for personal data breach and incident management, and
  - h. protocols for imparting privacy training to personnel.



**iv. BSPs should have robust grievance redress channels for customers.**

BSPs must—<sup>ccxxviii</sup>

- Have effective, efficient, speedy and time-bound grievance redress mechanisms that can help customers resolve data-related grievances.
- Publish details of the grievance redress officer and the data protection officer clearly in the privacy notice.
- The redress mechanisms should have simple procedures that do not burden customers.
- Customers should be able to seek redress through different digital and physical channels.
- BSPs could leverage AAs to retrieve details of transactions in dispute.
- BSPs should leverage technology to create better feedback loops with customers.





## CASE STUDY

### PRINCIPLE 9

# Demonstrating compliance with best data protection practices.

After receiving a series of messages concerning attempts to reset her password for her online digital banking app, Garima has reason to believe that someone is trying to use her personal data and contact details to breach her bank account. She contacts her BSP to notify them about the suspicious activity and safeguard her account. She soon realizes her account has been hacked and money has been transferred out of her account without her knowledge or authorization.

She tries to register a formal grievance with the BSP for not preventing the incident. The BSP denies any role in the incident claiming to have robust practices and rejects her complaint. Shortly after, reports surface about a major data breach from the BSP's technology partner's servers. The technology partner did not take sufficient measures to safeguard customers' passwords for the banking application from breaches and cyberattacks. When Garima approaches the Ombudsman, it becomes apparent that the BSP did not take adequate measures to ensure its partners maintained adequate data protection and security safeguards.

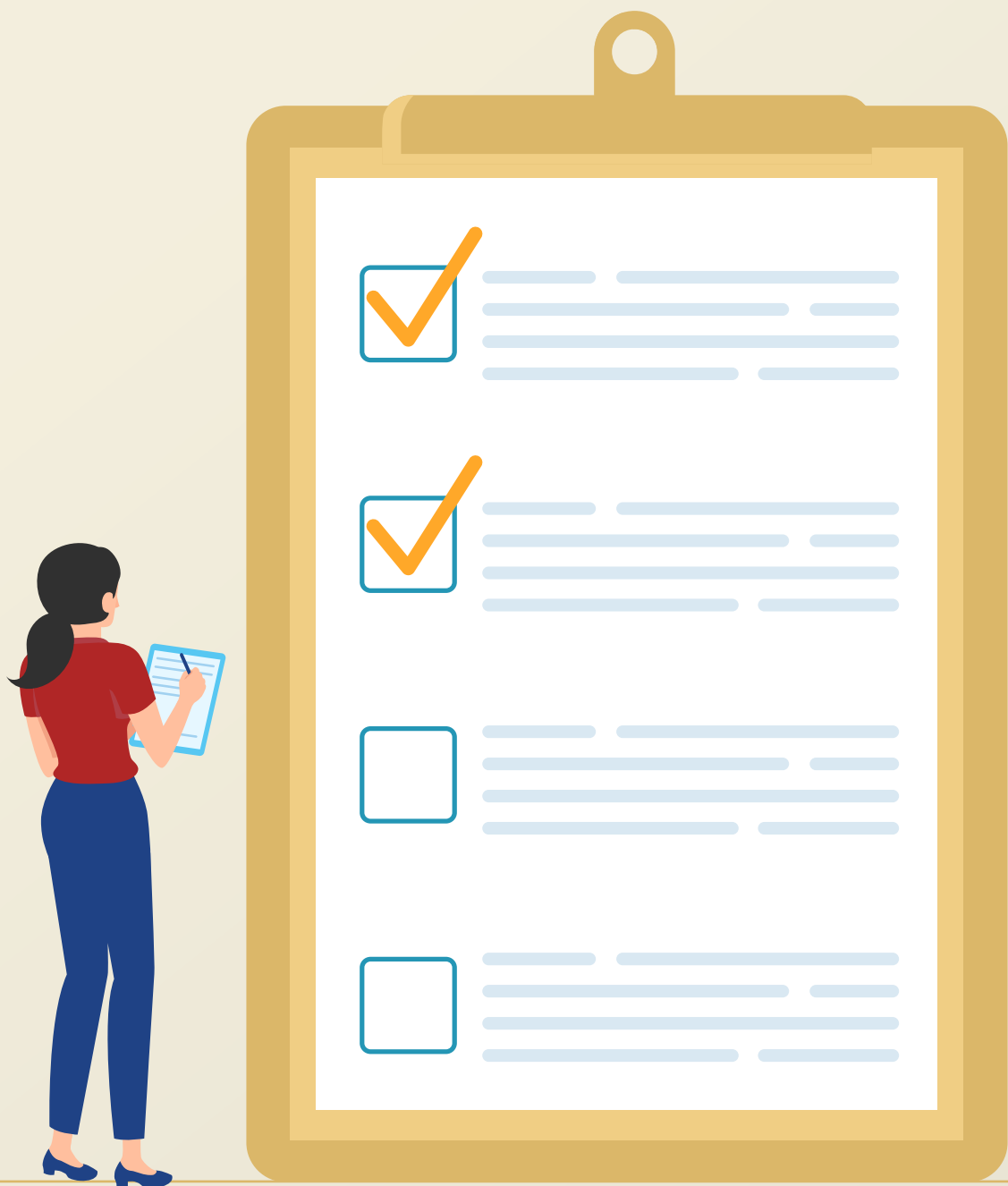
BSPs must be able to demonstrate that they and their partners comply with best data protection practices. For this, BSPs must –

- Establish procedures to ensure third parties have robust data protection and data security practices.
- Establish procedures including developing data protection policies, keeping records of data processing activities, auditing data protection practices etc.
- Create capacity within the organization and appoint personnel to engage with data protection-related queries and concerns from customers.
- Create robust grievance redress channels that can effectively and speedily provide redress to customers and to help BSPs identify vulnerabilities in their systems and practices.



6

SELF-ASSESSMENT  
CHECKLIST





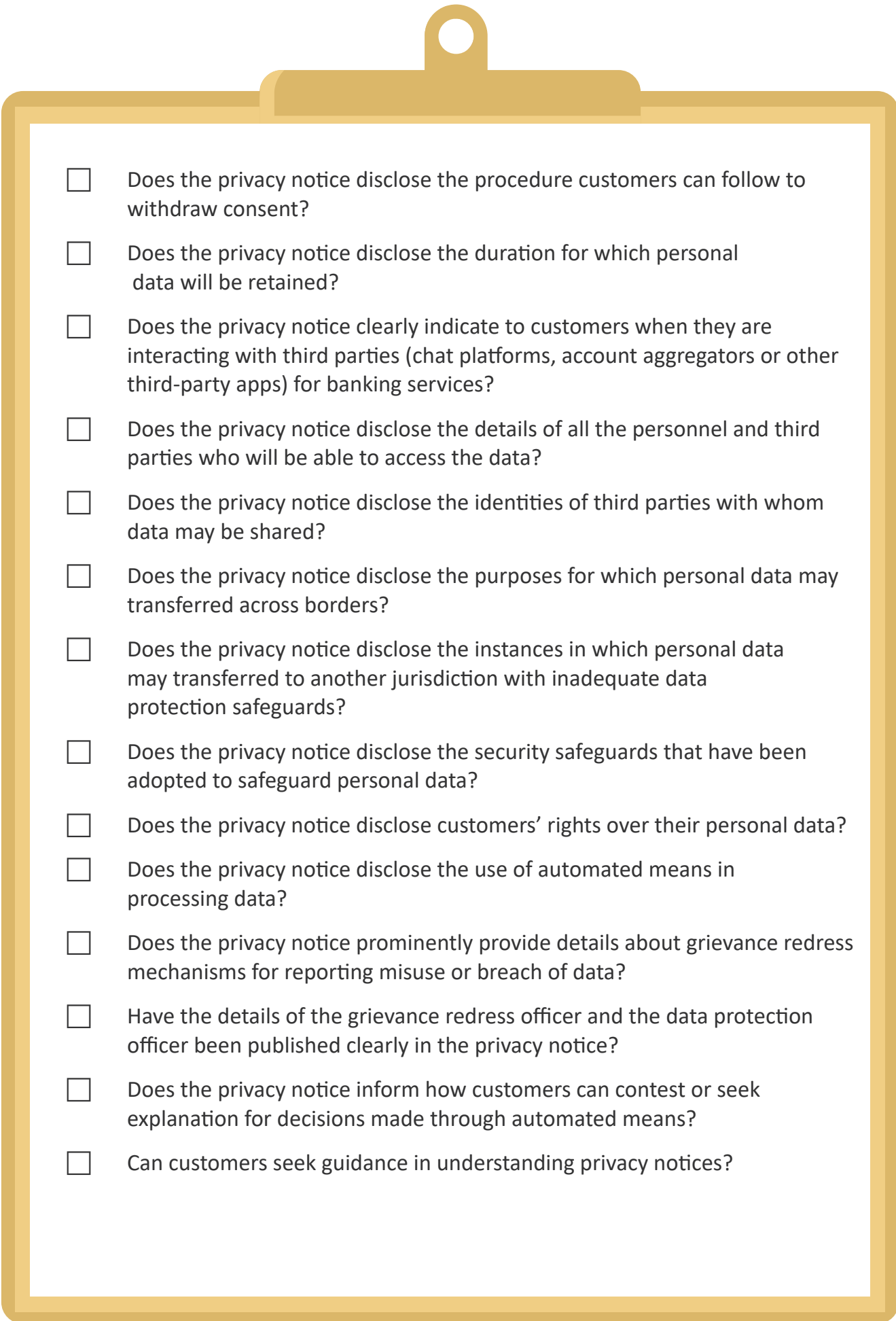
## **PRINCIPLE 1:**

# **SEGREGATING PERSONAL DATA AND ENSURING VISIBILITY OVER PERSONAL DATA.**

- 
- ☐ Does the BSP have policies for identifying and segregating different kinds of personal data?
  - ☐ Can the BSP segregate between personal data collected directly from customers, and indirectly from other sources?
  - ☐ Can the BSP segregate between personal data collected for primary and secondary purposes?
  - ☐ Does the BSP have an inventory of all processes and functions involving personal data?
  - ☐ Is the personal data inventory frequently revised and updated?
  - ☐ Does the BSP map personal data that is involved in each process and function?
  - ☐ Does the BSP have an inventory of third parties and partners with who personal data is shared?
  - ☐ Does the BSP map personal data that is shared with each third party and partner?
  - ☐ Does the BSP map its staff personnel's access to personal data?
  - ☐ Does the BSP map third parties' access to personal data?
  - ☐ Does the BSP map the flow of personal data to third parties?
  - ☐ Does the BSP map the technical assets involved in processing personal data?
  - ☐ Does the BSP define how personal data will be stored?
  - ☐ Does the BSP store personal data collected from different sources separately?
  - ☐ Has the BSP defined the level of protection and security different kinds of personal data will receive?
  - ☐ Can the BSP determine the personal data that must be pseudonymised and personal data that must be anonymised?

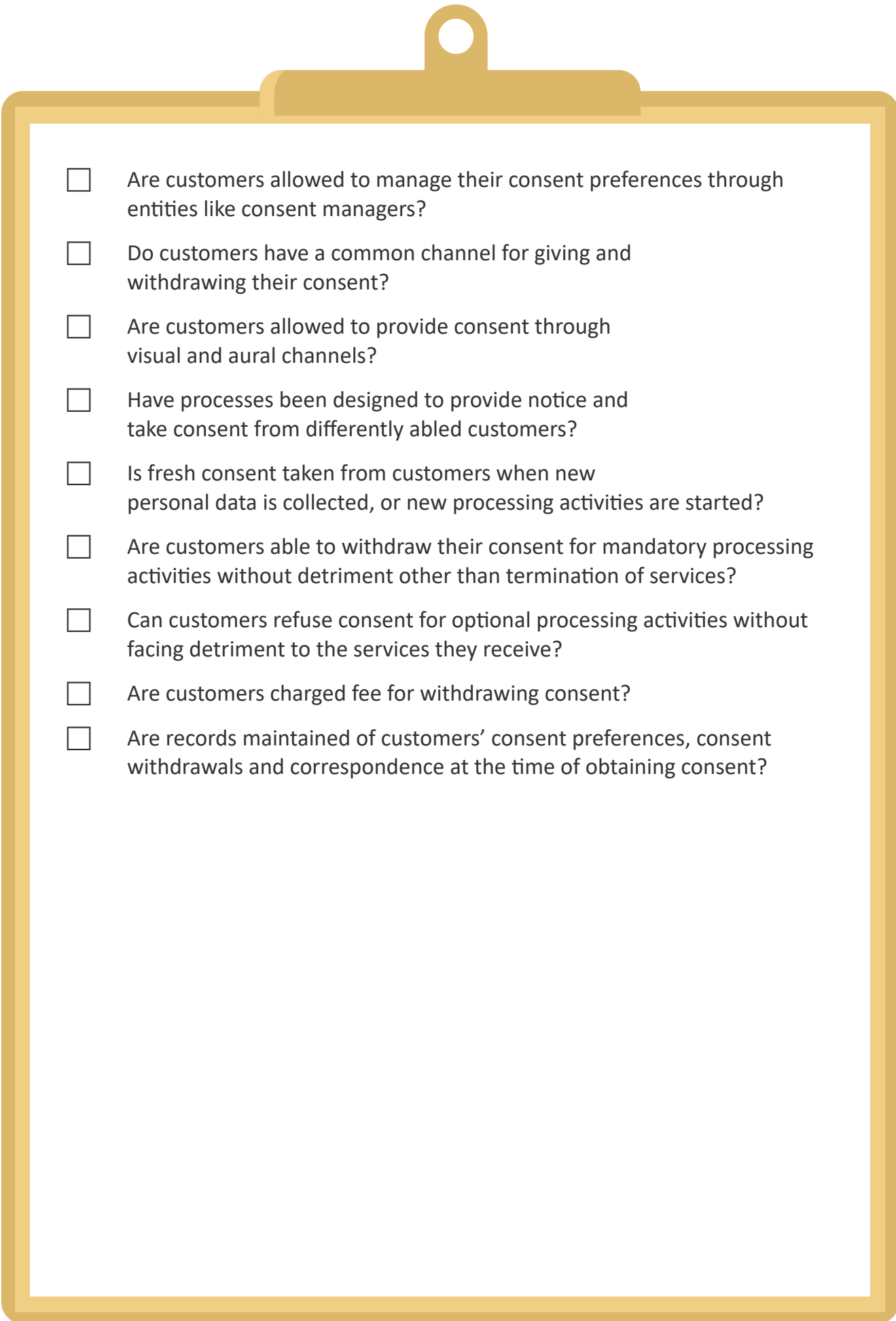
**PRINCIPLE 2:****COMMUNICATING EFFECTIVELY  
WITH CUSTOMERS.**

- 
- ☐ Does the BSP provide a privacy notice to the customer?
  - ☐ Is the privacy notice drafted in the preferred language of the customer?
  - ☐ Is the privacy notice written concisely?
  - ☐ Is there an aural privacy notice available for those unable to read?
  - ☐ Is the privacy notice written in simple, plain and easily understandable language?
  - ☐ Is the privacy notice presented just before data collection?
  - ☐ Does the privacy notice prominently disclose the purposes for processing personal data?
  - ☐ Is the purpose communicated in the privacy notice clear, specific, and lawful?
  - ☐ Are the provisions that request consent from customers placed distinctly from the other provisions in the notice?
  - ☐ Does the privacy notice disclose the types of personal data that will be collected directly from the customer?
  - ☐ Does the privacy notice disclose the types of personal data that will be collected indirectly from third parties?
  - ☐ Does the privacy notice disclose the types of data that are mandatory for a processing activity?
  - ☐ Does the privacy notice distinctly disclose the types of data that are optional for a processing activity?
  - ☐ Does the privacy notice disclose the implications for customers if they do not provide personal data?

- 
- ☐ Does the privacy notice disclose the procedure customers can follow to withdraw consent?
  - ☐ Does the privacy notice disclose the duration for which personal data will be retained?
  - ☐ Does the privacy notice clearly indicate to customers when they are interacting with third parties (chat platforms, account aggregators or other third-party apps) for banking services?
  - ☐ Does the privacy notice disclose the details of all the personnel and third parties who will be able to access the data?
  - ☐ Does the privacy notice disclose the identities of third parties with whom data may be shared?
  - ☐ Does the privacy notice disclose the purposes for which personal data may be transferred across borders?
  - ☐ Does the privacy notice disclose the instances in which personal data may be transferred to another jurisdiction with inadequate data protection safeguards?
  - ☐ Does the privacy notice disclose the security safeguards that have been adopted to safeguard personal data?
  - ☐ Does the privacy notice disclose customers' rights over their personal data?
  - ☐ Does the privacy notice disclose the use of automated means in processing data?
  - ☐ Does the privacy notice prominently provide details about grievance redress mechanisms for reporting misuse or breach of data?
  - ☐ Have the details of the grievance redress officer and the data protection officer been published clearly in the privacy notice?
  - ☐ Does the privacy notice inform how customers can contest or seek explanation for decisions made through automated means?
  - ☐ Can customers seek guidance in understanding privacy notices?

**PRINCIPLE 3:****OBTAINING INFORMED CONSENT FROM CUSTOMERS.**

- 
- ☐ Have customers been given all the information about how their personal data will be processed?
  - ☐ Have customers been given information about primary and secondary purposes for processing personal data?
  - ☐ Are customers informed of the potential risks from giving consent?
  - ☐ Are customers informed of measures that have been taken to mitigate risks to personal data?
  - ☐ Are customers informed of the use of automated systems for providing products and services?
  - ☐ Have the customers been briefed about the rationale, implications and intended effects of processing personal data through automated means?
  - ☐ Do any of the terms and conditions in the notice make it hard for customers to give consent freely?
  - ☐ Can customers seek guidance in understanding the implications of giving consent?
  - ☐ Is consent taken expressly from customers?
  - ☐ Are customers allowed to give consent separately for the different purposes of processing personal data?
  - ☐ Are customers allowed to withdraw their consent as easily as they were able to give consent?
  - ☐ Are customers able to verify and audit who BSPs shared their personal data with?
  - ☐ Can the BSP demonstrate that the consent they took from customers is informed, free, clear, express, specific, withdrawable, and auditable?

- 
- ☐ Are customers allowed to manage their consent preferences through entities like consent managers?
  - ☐ Do customers have a common channel for giving and withdrawing their consent?
  - ☐ Are customers allowed to provide consent through visual and aural channels?
  - ☐ Have processes been designed to provide notice and take consent from differently abled customers?
  - ☐ Is fresh consent taken from customers when new personal data is collected, or new processing activities are started?
  - ☐ Are customers able to withdraw their consent for mandatory processing activities without detriment other than termination of services?
  - ☐ Can customers refuse consent for optional processing activities without facing detriment to the services they receive?
  - ☐ Are customers charged fee for withdrawing consent?
  - ☐ Are records maintained of customers' consent preferences, consent withdrawals and correspondence at the time of obtaining consent?

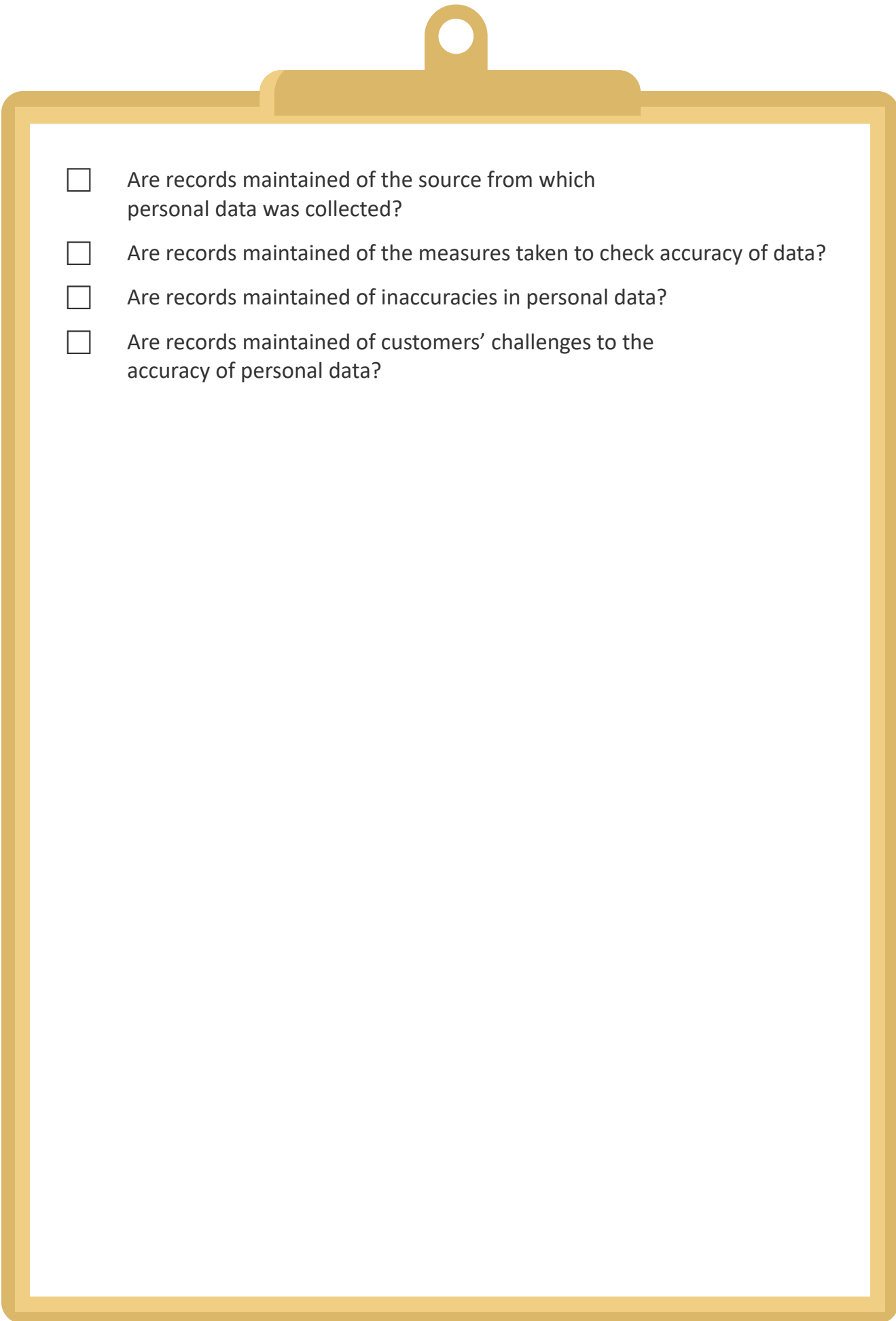




**PRINCIPLE 4:**

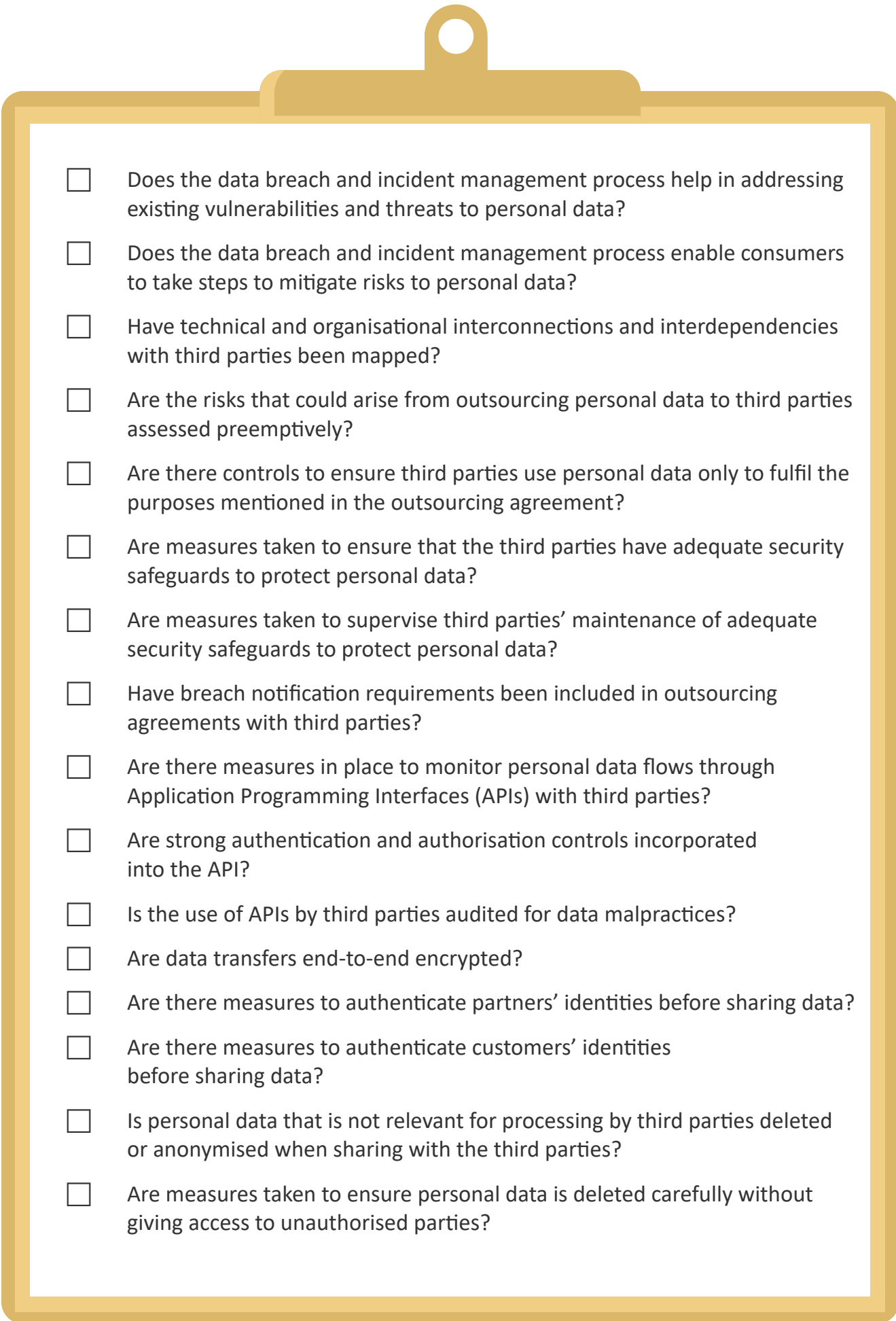
**COLLECTING ACCURATE AND PROPORTIONATE PERSONAL DATA FOR PROVIDING BANKING SERVICES.**

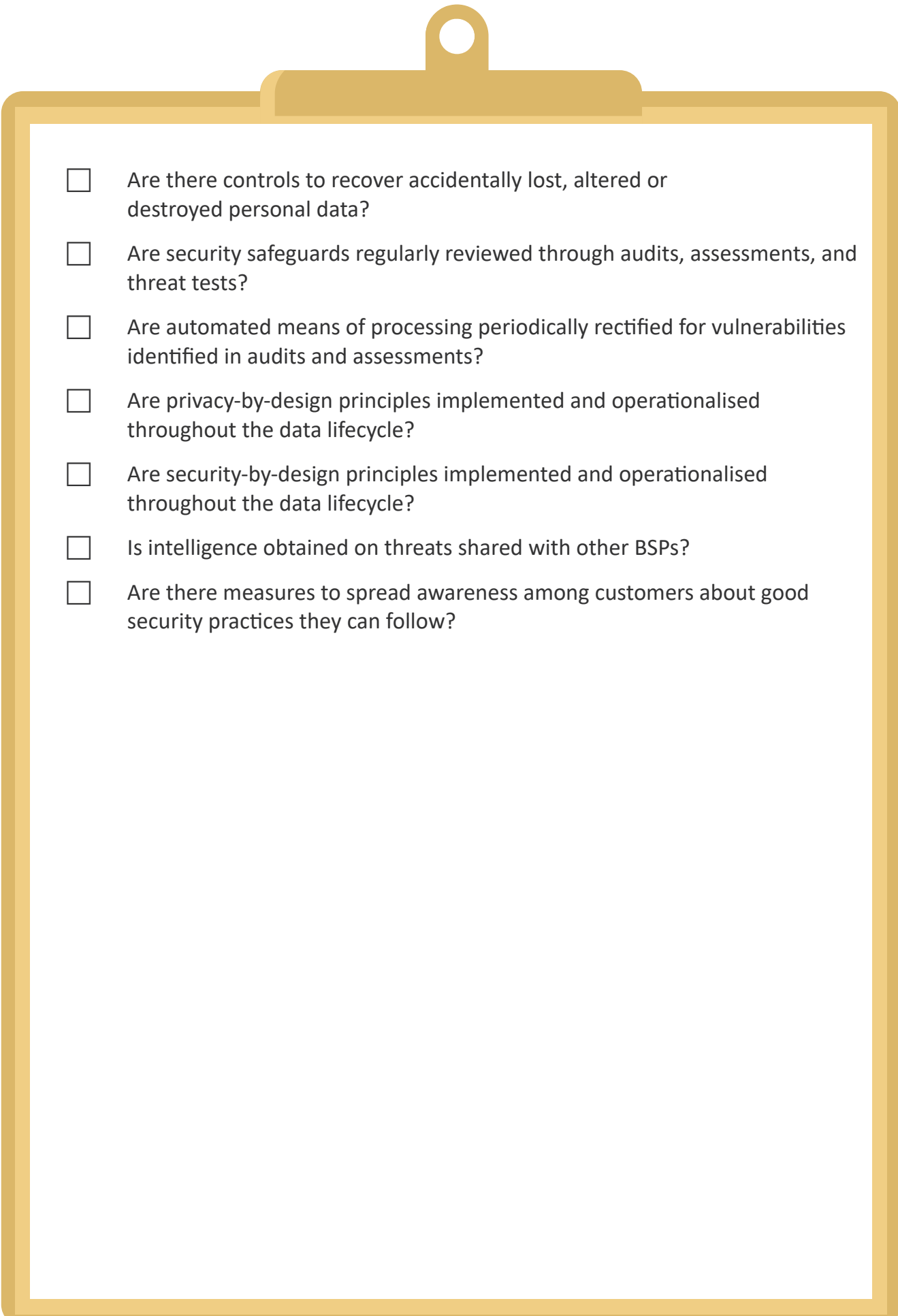
- 
- ☐ Is the personal data processed necessary for the purpose of processing?
  - ☐ Is the personal data processed relevant for the purpose of processing?
  - ☐ Is the data used for processing accurate, complete, representative, unbiased and up to date?
  - ☐ Is unnecessary personal data deleted promptly?
  - ☐ Is the personal data collected with the customers' consent?
  - ☐ Is the personal data collected through lawful means?
  - ☐ Is new personal data collected only when it is necessary for maintaining data accuracy or for fulfilling a purpose?
  - ☐ Are data protection impact assessments (DPIA) conducted to ensure proportionate personal data in processing?
  - ☐ Is quality of personal data frequently assessed for the purposes of processing?
  - ☐ Are there mechanisms to filter out incomplete, inaccurate, or unnecessary personal data during data collection?
  - ☐ Are there protocols for assessing the quality of data collected from third parties?
  - ☐ When using automated means, is the quality of outputs reviewed regularly when they are used for further processing activities?
  - ☐ Are there measures to review the processing activities to identify and rectify causes of bad data quality?
  - ☐ Are there mechanisms to identify and rectify inaccuracies and alterations in person data caused due to breach or cyberattack?

- 
- ☐ Are records maintained of the source from which personal data was collected?
  - ☐ Are records maintained of the measures taken to check accuracy of data?
  - ☐ Are records maintained of inaccuracies in personal data?
  - ☐ Are records maintained of customers' challenges to the accuracy of personal data?

**PRINCIPLE 5:****SECURING CUSTOMERS' PERSONAL DATA.**

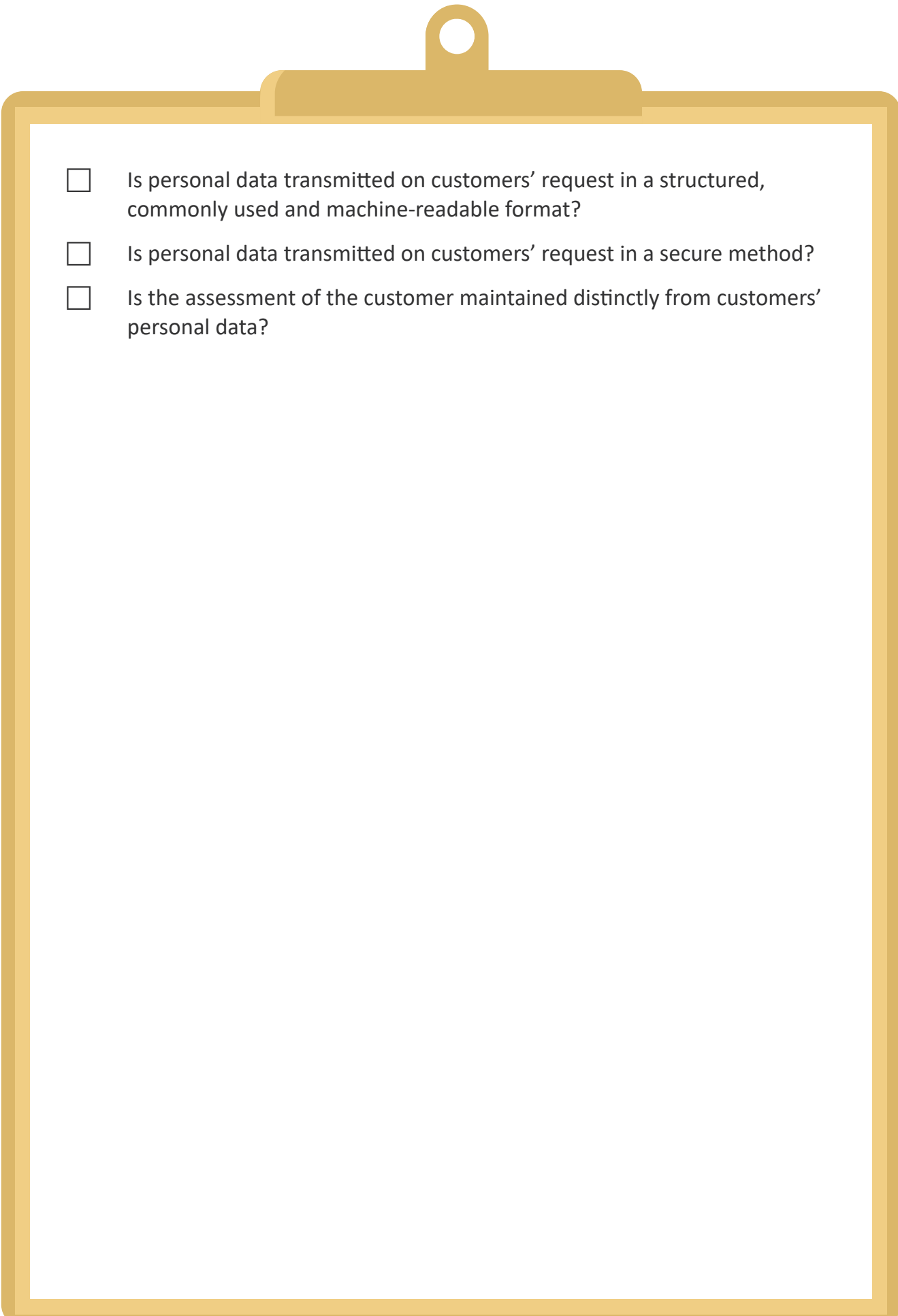
- 
- ☐ Is the technical infrastructure up-to-date and without any security or design flaws?
  - ☐ Are information audits conducted to assess inventory of the personal data?
  - ☐ Is the personal data inventory frequently revised and updated?
  - ☐ Are information audits conducted to understand vulnerabilities and risks to personal data?
  - ☐ Are risk assessments and threat tests conducted to understand risks to personal data?
  - ☐ Are the data protection impact assessments (DPIAs) and threat analyses conducted before using new technology for processing personal data?
  - ☐ Have anonymisation and deidentification techniques been implemented to secure personal data?
  - ☐ Are anonymised datasets reviewed continuously for the risk of reidentification?
  - ☐ Have technological measures, including encryption and passwords, been adopted for personal data protection?
  - ☐ Have organisational measures, including measures to ensure oversight and control, accountability, and data access, authentication and authorisation protocols been adopted for personal data protection?
  - ☐ Does the BSP undertake periodic evaluation of these measures?
  - ☐ Have physical measures, including security clearances to personal data servers, been adopted for personal data protection?
  - ☐ Are data protection guarantees in the privacy notice operationalised through security safeguards?
  - ☐ Has a data breach and incident management process been established?

- 
- ☐ Does the data breach and incident management process help in addressing existing vulnerabilities and threats to personal data?
  - ☐ Does the data breach and incident management process enable consumers to take steps to mitigate risks to personal data?
  - ☐ Have technical and organisational interconnections and interdependencies with third parties been mapped?
  - ☐ Are the risks that could arise from outsourcing personal data to third parties assessed preemptively?
  - ☐ Are there controls to ensure third parties use personal data only to fulfil the purposes mentioned in the outsourcing agreement?
  - ☐ Are measures taken to ensure that the third parties have adequate security safeguards to protect personal data?
  - ☐ Are measures taken to supervise third parties' maintenance of adequate security safeguards to protect personal data?
  - ☐ Have breach notification requirements been included in outsourcing agreements with third parties?
  - ☐ Are there measures in place to monitor personal data flows through Application Programming Interfaces (APIs) with third parties?
  - ☐ Are strong authentication and authorisation controls incorporated into the API?
  - ☐ Is the use of APIs by third parties audited for data malpractices?
  - ☐ Are data transfers end-to-end encrypted?
  - ☐ Are there measures to authenticate partners' identities before sharing data?
  - ☐ Are there measures to authenticate customers' identities before sharing data?
  - ☐ Is personal data that is not relevant for processing by third parties deleted or anonymised when sharing with the third parties?
  - ☐ Are measures taken to ensure personal data is deleted carefully without giving access to unauthorised parties?

- 
- ☐ Are there controls to recover accidentally lost, altered or destroyed personal data?
  - ☐ Are security safeguards regularly reviewed through audits, assessments, and threat tests?
  - ☐ Are automated means of processing periodically rectified for vulnerabilities identified in audits and assessments?
  - ☐ Are privacy-by-design principles implemented and operationalised throughout the data lifecycle?
  - ☐ Are security-by-design principles implemented and operationalised throughout the data lifecycle?
  - ☐ Is intelligence obtained on threats shared with other BSPs?
  - ☐ Are there measures to spread awareness among customers about good security practices they can follow?

**PRINCIPLE 6:****USING OR DISCLOSING PERSONAL DATA WITH THE CONSENT OF THE CUSTOMER.**

- 
- ☐ Is there a list of third parties to whom personal data maybe disclosed maintained?
  - ☐ Has the customer been provided with a standard list of third parties to whom personal data may be disclosed?
  - ☐ Is there a list of purposes for which personal data may be shared to third parties disclosed to customers?
  - ☐ Have personal data disclosures to third parties stopped after a customer has withdrawn consent?
  - ☐ Have mechanisms been installed to receive and record data porting requests from customers?
  - ☐ Are there organisation-level policies to recognise and operationalise data porting requests?
  - ☐ Has capacity been developed in the organisation to recognise and operationalise data porting requests?
  - ☐ Have measures been adopted to respond to porting requests in a timely manner?
  - ☐ Has the identity of the requesting customer been verified before transmitting data?
  - ☐ Have measures been adopted to receive and transmit personal data to third parties on customers' requests ?
  - ☐ Can customers request for porting information at reasonable cost?
  - ☐ Is personal data transmitted on customers' request without placing legal or technical obstacles?

- 
- ☐ Is personal data transmitted on customers' request in a structured, commonly used and machine-readable format?
  - ☐ Is personal data transmitted on customers' request in a secure method?
  - ☐ Is the assessment of the customer maintained distinctly from customers' personal data?

**PRINCIPLE 7:****ENABLING CUSTOMERS TO ACCESS AND RECTIFY THEIR PERSONAL DATA.**

- 
- ☐ Are personal data access and rectification processes clearly communicated to customers?
  - ☐ Are customers able to access their own personal data in a structured, machine-readable format?
  - ☐ Are customers able to access and rectify their personal data collected indirectly from third parties?
  - ☐ Are customers able to access and rectify their personal data when they choose to without cost or delay?
  - ☐ Do customers have the choice to rectify personal data through different physical and digital channels?
  - ☐ Have changes been made to all personal data records to match the modifications made by customers?
  - ☐ Have measures been taken to ensure that third parties rectify their personal data records?
  - ☐ Have amended personal data records been provided to third parties after customers have made changes?



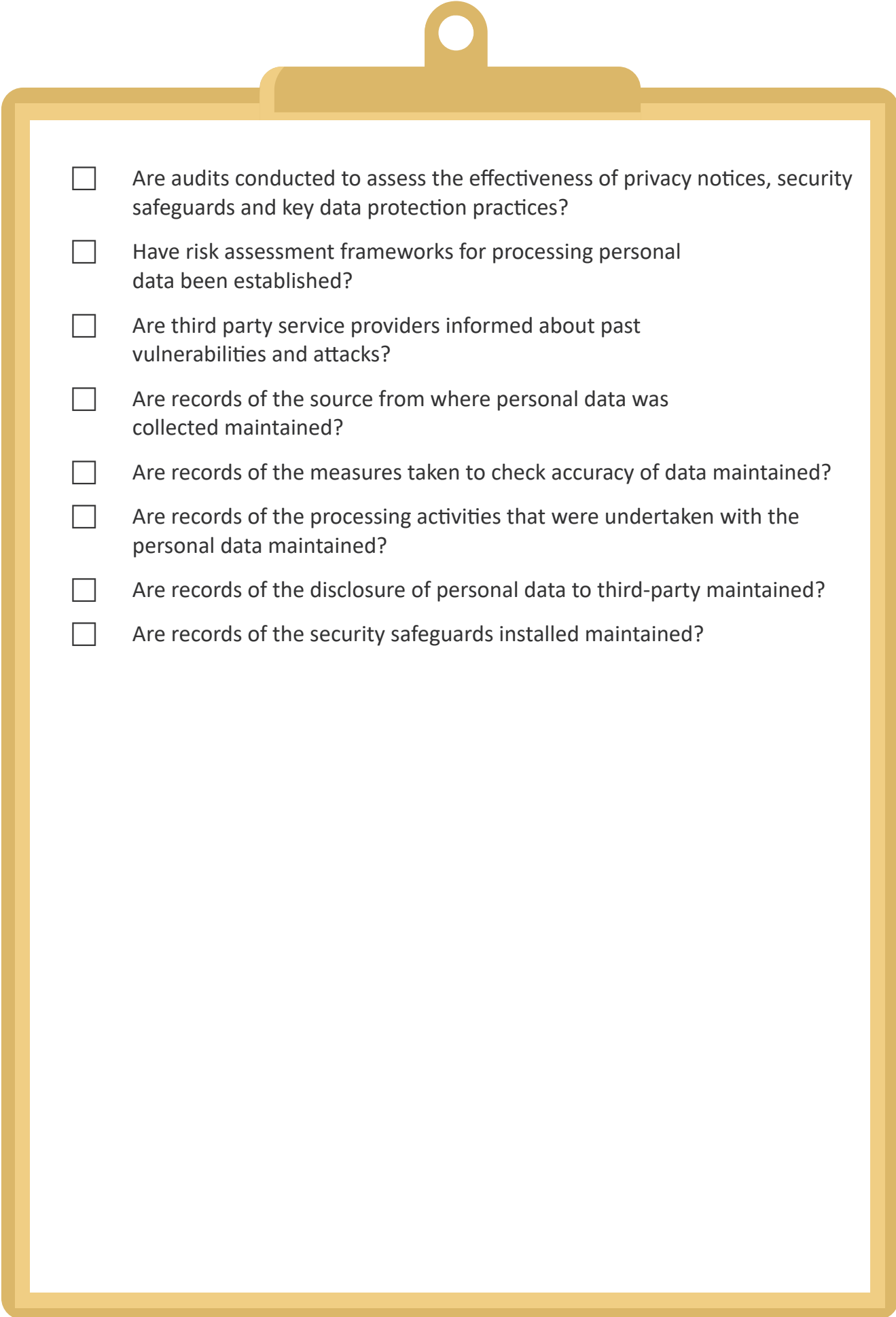
**PRINCIPLE 8:****USING AUTOMATED MEANS OF PROCESSING RESPONSIBLY.**

- 
- ☐ Are there measures to ensure transparency, auditability, accountability and explainability of decisions made by automated means?
  - ☐ Can the factors and processes used by the automated means be explained in simple, clear and comprehensible terms to customers?
  - ☐ Are there records of the actions taken to identify, document and mitigate risks from automated means to customers' rights?
  - ☐ Are there records of the datasets and processes used by automated means to arrive at decisions?
  - ☐ Have the automated means of processing been sandboxed or piloted to preemptively identify risks to customers?
  - ☐ Are the automated means designed to be fit for the purpose of processing?
  - ☐ Has the robustness and security of automated means been tested before being put into use?
  - ☐ Have the reliability and accuracy of outputs produced by the automated means been tested before being put into use?
  - ☐ Has it been demonstrated that the automated means of processing provide legitimate outputs without discrimination?
  - ☐ Is the data being processed representative, unbiased and of high-quality?
  - ☐ Is the personal data that is being processed by automated means been de-biased?
  - ☐ Have the best standards been adopted for gathering and labelling personal data that will be used for processing by automated means?
  - ☐ Has bias in the decision-making process by automated means been identified and addressed?

- 
- ☐ Are automated means examined continually to identify vulnerabilities?
  - ☐ Have measures been adopted to mitigate the risks identified from automated means?
  - ☐ Are periodic audits conducted to identify vulnerabilities in the automated means of processing?
  - ☐ Are automated means monitored on an on-going basis?
  - ☐ Are the personnel who develop and administrate automated means trained to ensure responsible processing?
  - ☐ Are there effective management and oversight controls over third-party vendors providing automated means?
  - ☐ Have customers been notified through all service delivery channels that automated means may be used for making decisions about them?
  - ☐ Are customers able to contest decisions made through automated means?
  - ☐ Are customers able to submit complaints about decisions made through automated means?
  - ☐ Are customers able to contest or seek review of decisions made through automated means?
  - ☐ Are customers able to seek redress when their rights are harmed by processing by automated means?
  - ☐ Do customers have access to data management tools that can help them review, edit, and update personal data that is processed through automated means?
  - ☐ Have customers been made aware of their rights in relation to how their personal data is processed through automated means?

**PRINCIPLE 9:****DEMONSTRATING COMPLIANCE WITH BEST DATA PROTECTION PRACTICES.**

- 
- ☐ Are there protocols for collection of personal data?
  - ☐ Are there protocols for controlling access to personal data?
  - ☐ Are there protocols for retaining and deleting personal data?
  - ☐ Are there protocols for managing personal data breaches and other cyber incidents?
  - ☐ Are there protocols for imparting data-privacy training to personnel?
  - ☐ Are there data policies in place that define the means to ensure data quality?
  - ☐ Are there data policies in place that define security safeguards?
  - ☐ Are personnel trained to answer inquiries about the privacy policies, consent processes, security safeguards and redress processes?
  - ☐ Are personnel appointed for monitoring compliance with data protection law and ensure best practices in data protection?
  - ☐ Are the names of personnel responsible for data protection practices published for customers' reference?
  - ☐ Is there an effective, efficient, speedy and time-bound grievance redress mechanism in place that can help customers resolve data-related grievances?
  - ☐ Are the redress mechanisms simple?
  - ☐ Are customers able to seek redress through both digital and physical channels?
  - ☐ Have redress channels been leveraged to gain feedback directly from customers?

- 
- ☐ Are audits conducted to assess the effectiveness of privacy notices, security safeguards and key data protection practices?
  - ☐ Have risk assessment frameworks for processing personal data been established?
  - ☐ Are third party service providers informed about past vulnerabilities and attacks?
  - ☐ Are records of the source from where personal data was collected maintained?
  - ☐ Are records of the measures taken to check accuracy of data maintained?
  - ☐ Are records of the processing activities that were undertaken with the personal data maintained?
  - ☐ Are records of the disclosure of personal data to third-party maintained?
  - ☐ Are records of the security safeguards installed maintained?

# References

<sup>i</sup> RBI's Core Purpose, Values and Vision, Reserve Bank of India, [https://rbi.org.in/scripts/BS\\_RBIsCorePurpose.aspx](https://rbi.org.in/scripts/BS_RBIsCorePurpose.aspx); Protecting customers – Safeguarding stability, Reserve Bank of India, <https://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/AIBDAS170914.pdf>.

<sup>ii</sup> Reserve Bank of India, Charter of Customer Rights, 03 December 2014, [https://rbidocs.rbi.org.in/rdocs/content/pdfs/CCSR03122014\\_1.pdf](https://rbidocs.rbi.org.in/rdocs/content/pdfs/CCSR03122014_1.pdf).

<sup>iii</sup> See Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors, AIR 2017 SC 4161

<sup>iv</sup> See Mr. Khan Shakil Meer v. Bank of Maharashtra, CIC/SG/A/2011/002607/16168

<sup>v</sup> See Chairman and Managing Director, United Commercial Bank and Others v. P.C. Kakkar, (2003) 4 SCC 364; Asst. General Manager State Bank of India v. Ashok Kumar Bhatia, W.P. (C) 7584/2017 (Delhi High Court).

<sup>vi</sup> Financial Inclusion Index for India, Reserve Bank of India, 16 September 2021, [https://www.rbi.org.in/Scripts/BS\\_ViewBulletin.aspx?Id=20502#:~:text=A%20multidimensional%20composite%20Financial%20Inclusion,financial%20literacy%2C%20and%20consumer%20protection.](https://www.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=20502#:~:text=A%20multidimensional%20composite%20Financial%20Inclusion,financial%20literacy%2C%20and%20consumer%20protection.)

<sup>vii</sup> The Hindu BusinessLine Bureau, Over 5.82 crore Jan Dhan accounts inoperative: Finance Ministry, THE HINDU BUSINESSLINE, 10 August 2021, <https://www.thehindubusinessline.com/economy/over-582-crore-jan-dhan-accounts-inoperative-finance-ministry/article35832894.ece>; "India: Overview," Financial Inclusion Insights, accessed October 1, 2020, <http://finclusion.org/country/asia/india.html#overview>; "India: Data at a glance," Financial Inclusion Insights, accessed October 1, 2020, <http://finclusion.org/country/asia/india.html#dataAtAGlance>; Reserve Bank of India, "Report on Trend and Progress of Banking in India 2018-19," Reserve Bank of India, 2019, <https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/ORTP241219FL760D9F69321B47988DE44D68D9217A7E.PDF>; Anand Adhikari, "Jan Dhan Yojana data shows rural area residents using bank accounts more often," Business Today, November 20, 2019, <https://www.businesstoday.in/sectors/banks/zero-balance-dormant-bank-accounts-under-jan-dhan-yojana-on-a-steady-decline/story/390664.html>; The Hindu Business Line, "Almost every fifth Jan Dhan account 'inoperative'," The Hindu Business Line, February 6, 2020, <https://www.thehindubusinessline.com/money-and-banking/almost-every-fifth-jan-dhan-account-inoperative/article30754738.ece>.

<sup>viii</sup> PTI, Half of India's working population of 400 mn people credit active: Report, BUSINESS STANDARD, 29 June 2021, [https://www.business-standard.com/article/finance/half-of-india-s-working-population-of-400-mn-people-credit-active-report-121062900822\\_1.html](https://www.business-standard.com/article/finance/half-of-india-s-working-population-of-400-mn-people-credit-active-report-121062900822_1.html).

<sup>ix</sup> Payment System Indicators, Reserve Bank of India, May 2022, <https://rbidocs.rbi.org.in/rdocs/PSI/PDFs/PSIMAY2022F6402F5851B94DF5AFAABB98D08754AA.PDF>.

<sup>x</sup> Reserve Bank of India, Report of the Committee on Computerisation in Banks, 1984, [https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CR585\\_198968AC542798894FCA83FC8B0C8DB56262.PDF](https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CR585_198968AC542798894FCA83FC8B0C8DB56262.PDF); Payments System Group, "Payment Systems in India," RESERVE BANK OF INDIA, December 12, 2020, <https://www.rbi.org.in/Scripts/OccasionalPublications.aspx?head=Payment%20Systems%20in%20India>; Committee on Payment and Settlement System, "Payment, Clearing and Settlement Systems in the CPSS countries (Vol. 1)," BANK FOR INTERNATIONAL SETTLEMENTS, 2011, <https://www.bis.org/cpmi/publ/d97.pdf>; Shaji, A.M., Evolution and Growth of Digital Banking in India, ENTERSLICE, 12 September 2020, <https://enterslice.com/learning/evolution-and-growth-of-digital-banking-in-india/>.

<sup>xi</sup> Committee on Payment and Settlement System, "Payment, Clearing and Settlement Systems in the CPSS countries (Vol. 1)," Bank for International Settlements, 2011, <https://www.bis.org/cpmi/publ/d97.pdf>; Payments System Group, "Payment Systems in India," Reserve Bank of India, December 12, 2020, <https://www.rbi.org.in/Scripts/OccasionalPublications.aspx?head=Payment%20Systems%20in%20India>; Reserve Bank of India, "Vision 2001-03," Reserve Bank of India, n.d., [https://www.rbi.org.in/scripts/bs\\_viewcontent.aspx?Id=2179](https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=2179).

<sup>xii</sup> S.S. Mundra, "Information Technology & Cyber Risk in Banking Sector," RESERVE BANK OF INDIA, October 10, 2016, [https://www.rbi.org.in/scripts/BS\\_ViewBulletin.aspx?Id=16508](https://www.rbi.org.in/scripts/BS_ViewBulletin.aspx?Id=16508); Working Group on Electronic Banking, "Report of the Working Group on Electronic Banking," RESERVE BANK OF INDIA, January 21, 2011, [https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111\\_C9.pdf](https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111_C9.pdf).

<sup>xiii</sup> Reserve Bank of India, "Overview of Payment Systems in India. Retrieved from Reserve Bank of India," RESERVE BANK OF INDIA, n.d., [https://www.rbi.org.in/scripts/PaymentSystems\\_UM.aspx](https://www.rbi.org.in/scripts/PaymentSystems_UM.aspx).

<sup>xiv</sup> Reserve Bank of India, "Overview of Payment Systems in India. Retrieved from Reserve Bank of India," Reserve Bank of India, n.d., [https://www.rbi.org.in/scripts/PaymentSystems\\_UM.aspx](https://www.rbi.org.in/scripts/PaymentSystems_UM.aspx); "What We Do," National Payments Corporation of India, accessed October 1, 2020, <https://www.npci.org.in/node>; Malavika Raghavan, Beni Chugh, and Anubhuti Singh, "Primer on Consumer Data Infrastructure," Dvara Research, April 4, 2019, <https://www.dvara.com/research/conference2019/wp-content/uploads/2019/04/Primer-on-Consumer-Data-Infrastructure.pdf>.

<sup>xv</sup> Reserve Bank of India, Disruptions and Opportunities in the Financial Sector (Address by Shri Shaktikanta Das, Governor, Reserve Bank of India – June 17, 2022) – Delivered at the Financial Express Modern BFSI Summit in Mumbai, 17 June 2022, [https://www.rbi.org.in/Scripts/BS\\_SpeechesView.aspx?Id=1311](https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1311).

<sup>xvi</sup> Pradhan Mantri Jan Dhan Yojana, Department of Financial Services, Government of India, <https://pmjdy.gov.in/about>; Jan Dhan Yojana, Aadhaar and Mobile Connectivity (JAM) trinity, Digital India, <https://digitalindia.gov.in/ebook/dot/page6.php>.

<sup>xvii</sup> “What We Do,” National Payments Corporation of India, accessed October 1, 2020, <https://www.npci.org.in/node>; Government of India, “Digital Payment Methods,” Cashless India, n.d., [http://cashlessindia.gov.in/digital\\_payment\\_methods.html](http://cashlessindia.gov.in/digital_payment_methods.html).

<sup>xviii</sup> Chugh, B., Raghavan, M. and Singh, M., Primer on Designing Optimal Regulation, DVARA RESEARCH, 1 April 2019, <https://www.dvara.com/research/conference2019/wp-content/uploads/2019/04/Primer-on-Consumer-Data-Infrastructure.pdf>; Chen, S., D’Silva, D.; Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, <https://www.bis.org/publ/bppdf/bisap120.pdf>.

<sup>xix</sup> Tracxn, Top alternative credit score provider startups, 16 April 2022, <https://tracxn.com/d/trending-themes/Startups-in-Alternative-Credit-Score-Providers>.

<sup>xx</sup> Team TMS, What is a neobank?, BUSINESS STANDARD, 06 May 2022, [https://www.business-standard.com/podcast/finance/what-is-a-neobank-122050600048\\_1.html#:~:text=A%20neobank%20is%20a%20digital,under%20the%20umbrella%20of%20neobanking..](https://www.business-standard.com/podcast/finance/what-is-a-neobank-122050600048_1.html#:~:text=A%20neobank%20is%20a%20digital,under%20the%20umbrella%20of%20neobanking..)

<sup>xxi</sup> Chugh, B., Raghavan, M. and Singh, M., Primer on Designing Optimal Regulation, DVARA RESEARCH, 1 April 2019, <https://www.dvara.com/research/conference2019/wp-content/uploads/2019/04/Primer-on-Consumer-Data-Infrastructure.pdf>; Chen, S., D’Silva, D.; Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, <https://www.bis.org/publ/bppdf/bisap120.pdf>.

<sup>xxii</sup> Reserve Bank of India, Disruptions and Opportunities in the Financial Sector (Address by Shri Shaktikanta Das, Governor, Reserve Bank of India – June 17, 2022) – Delivered at the Financial Express Modern BFSI Summit in Mumbai, 17 June 2022, [https://www.rbi.org.in/Scripts/BS\\_SpeechesView.aspx?Id=1311](https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1311).

<sup>xxiii</sup> Chen, S., D’Silva, D.; Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, <https://www.bis.org/publ/bppdf/bisap120.pdf>.

<sup>xxiv</sup> D. Medine, F. Montes, Data Protection and Privacy for Alternative Data, WORLD BANK AND CGAP, (2018), [https://www.gpfi.org/sites/gpfi/files/documents/Data\\_Protection\\_and\\_Privacy\\_for\\_Alternative\\_Data\\_WBG.pdf](https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf); OECD, Technology and innovation in the insurance sector, OECD, (2017), <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf>.

<sup>xxv</sup> Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, BANK FOR INTERNATIONAL SETTLEMENTS, November 2019, available at <https://www.bis.org/bcbs/publ/d486.pdf>; Rathi, A. and Mohandas, S., FinTech in India: A study of privacy and security commitments, THE CENTRE FOR INTERNET AND SOCIETY, April 2019, available at <https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf>.

<sup>xxvi</sup> D. Medine, F. Montes, Data Protection and Privacy for Alternative Data, WORLD BANK AND CGAP, (2018), [https://www.gpfi.org/sites/gpfi/files/documents/Data\\_Protection\\_and\\_Privacy\\_for\\_Alternative\\_Data\\_WBG.pdf](https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf); OECD, Technology and innovation in the insurance sector, OECD, (2017), <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf>.

<sup>xxvii</sup> Beck, T., Cecchetti, S., Grothe, M., Kemp, M., Pelizzon, L. and Serrano, A.S., Will video kill the radio star? – Digitalisation and the future of banking, EUROPEAN SYSTEMIC RISK BOARD, January 2022, [https://www.esrb.europa.eu/pub/pdf/asc/esrb.ascreport202201\\_digitalisationandthefutureofbanking~83f079b5c7.en.pdf?87d77f9d8be17bcd1c5bacb79455b1f0](https://www.esrb.europa.eu/pub/pdf/asc/esrb.ascreport202201_digitalisationandthefutureofbanking~83f079b5c7.en.pdf?87d77f9d8be17bcd1c5bacb79455b1f0).

<sup>xxviii</sup> Chen, S., D’Silva, D.; Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, <https://www.bis.org/publ/bppdf/bisap120.pdf>; Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>.

<sup>xxix</sup> Chen, S., D’Silva, D.; Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, <https://www.bis.org/publ/bppdf/bisap120.pdf>; Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>.

<sup>xxx</sup> Singh, A. and Prasad, S., Artificial Intelligence in Digital Credit in India, DVARA RESEARCH, 13 April 2020, <https://www.dvara.com/research/blog/2020/04/13/artificial-intelligence-in-digital-credit-in-india/>.

<sup>xxxi</sup> Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>.

<sup>xxxii</sup> Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>.

<sup>xxxiii</sup> Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>.

<sup>xxxiv</sup> Consumer Financial Protection Bureau, CFPB Explores Impact of Alternative Data on Credit Access for Consumers who are credit invisible, 16 February 2017, <https://www.consumerfinance.gov/about-us/newsroom/cfpb-explores-impact-alternative-data-credit-access-consumers-who-are-credit-invisible/>; Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>; Singh, A., Raghavan, M. and Chugh, B., Primer on Consumer Data Regulation,

DVARA RESEARCH, 1 April 2019, <https://www.dvara.com/research/conference2019/wp-content/uploads/2019/04/Primer-on-Consumer-Data-Regulation.pdf>.

<sup>xxxv</sup> Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>.

- <sup>xxxvi</sup> Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Report and Recommendations, RESERVE BANK OF INDIA, January 2011, <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf>.
- <sup>xxxvii</sup> Chen, S., D'Silva, D.; Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, <https://www.bis.org/publ/bppdf/bispap120.pdf>.
- <sup>xxxviii</sup> Chen, S., D'Silva, D.; Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, <https://www.bis.org/publ/bppdf/bispap120.pdf>.
- <sup>xxxix</sup> Nariyanuri, S.S., Mobile payment apps driving Fintech Frenzy in India, S&P GLOBAL, 09 May 2019, <https://www.spglobal.com/marketintelligence/en/news-insights/blog/mobile-payment-apps-driving-fintech-frenzy-in-india>.
- <sup>xl</sup> Reserve Bank of India, Establishment of Digital Banking Units (DBUs), 07 April 2022, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12285&Mode=0>.
- <sup>xli</sup> Reserve Bank of India, Regulatory Sandbox (RS): First Cohort on 'Retail Payments' – Exit, 13 September 2021, [https://www.rbi.org.in/Scripts/BS\\_PressReleaseDisplay.aspx?prid=52217](https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52217); Reserve Bank of India, Regulatory Sandbox (RS): Second Cohort on Cross Border Payments – Test Phase, 13 September 2021, [https://www.rbi.org.in/Scripts/BS\\_PressReleaseDisplay.aspx?prid=52218](https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52218).
- <sup>xlii</sup> Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors, AIR 2017 SC 4161
- <sup>xliii</sup> See S. Sengupta, Financial Data Protection in Indian Regulatory Policy: From 'Secrecy' and 'Confidentiality' to 'Privacy', JOURNAL OF INDIAN LAW AND SOCIETY, 12(1), 86, (2021), retrieved from: <https://jils.co.in/wp-content/uploads/2021/06/Financial-Data-Protections.pdf> (Sengupta, 2021).
- <sup>xliv</sup> Ministry of Electronics and Information Technology, the Digital Personal Data Protection Bill of 2022, retrieved from: <https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022> (DPDPB 2022).
- <sup>lv</sup> S. Kakkar, New Digital Personal Data Protection Bill 'at the earliest', Centre tells SC, The New Indian Express, (2022), retrieved from: <https://www.newindianexpress.com/nation/2023/jan/17/new-digital-personal-data-protection-bill-at-the-earliest-centretells-sc-2538743.html>
- <sup>lvi</sup> Reserve Bank of India, "Cyber Security Framework in Banks," Reserve Bank of India, June 02, 2016, <https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=10435>; Reserve Bank of India, "Guidelines on Regulation of Payment Aggregators and Payment Gateways," Reserve Bank of India, March 17, 2020, <https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11822>; Reserve Bank of India, Disruptions and Opportunities in the Financial Sector (Address by Shri Shaktikanta Das, Governor, Reserve Bank of India – June 17, 2022) – Delivered at the Financial Express Modern BFSI Summit in Mumbai, 17 June 2022, [https://www.rbi.org.in/Scripts/BS\\_SpeechesView.aspx?Id=1311](https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1311).
- <sup>lvii</sup> Reserve Bank of India, Disruptions and Opportunities in the Financial Sector (Address by Shri Shaktikanta Das, Governor, Reserve Bank of India – June 17, 2022) – Delivered at the Financial Express Modern BFSI Summit in Mumbai, 17 June 2022, [https://www.rbi.org.in/Scripts/BS\\_SpeechesView.aspx?Id=1311](https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1311); Reserve Bank of India, Guidelines on Digital Lending, 2 September 2022, <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF>; Reserve Bank of India, Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022, 21 April 2022, Reserve Bank of India, Guidelines on Digital Lending, 2 September 2022, <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF>.
- <sup>lviii</sup> Reserve Bank of India, Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016, 02 September 2016, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598>.
- <sup>lix</sup> Reserve Bank of India, Guidelines on Digital Lending, 2 September 2022, <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF>.
- <sup>i</sup> Reserve Bank of India, Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions (2022), retrieved from: [https://rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=12300](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12300)
- <sup>ii</sup> See Reserve Bank of India, Report on Trend and Progress of Banking in India 2020-21, 123, (2021) available at: <https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/ORTP2020CF9C9E7D1DE44B1686906D7E3EF36F13.PDF>
- <sup>iii</sup> Id.
- <sup>iiii</sup> See Reserve Bank of India, Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs, (2021), available at: <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12179&Mode=0>
- <sup>lv</sup> L. Datwani, A. Rahman, India's New Approach to Personal Data Sharing, Consultative Group to Assist the Poor (CGAP), (2020) available at [https://www.cgap.org/sites/default/files/publications/2020\\_07\\_Working\\_Paper\\_India\\_New\\_Approach\\_Personal\\_Data\\_Sharing.pdf](https://www.cgap.org/sites/default/files/publications/2020_07_Working_Paper_India_New_Approach_Personal_Data_Sharing.pdf)
- <sup>lv</sup> M. Raghavan, A. Singh, Regulation of information flows as Central Bank functions? Implications from the treatment of Account Aggregators by the Reserve Bank of India, 2020 Central Bank of the Future Conference, (2020) available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3924793](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3924793)
- <sup>lvi</sup> See Reserve Bank of India, All you wanted to know about NBFCs, (2017) available at: <https://rbi.org.in/Scripts/FAQView.aspx?Id=92>
- <sup>lvii</sup> See Section 5, Credit Information Companies Act of 2005.
- <sup>lviii</sup> See Section 215, IBC. Also see, RBI, Submission of Financial Information to Information Utilities, (2017) retrieved from: <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11189>



<sup>lix</sup> For details on entities authorized to act as payment system operators in India, see Reserve Bank of India, Certificates of Authorization issued by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for Setting up and Operating Payment System in India, (2022), available at: <https://m.rbi.org.in/scripts/publicationsview.aspx?id=12043>

<sup>lx</sup> See Department of Economic Affairs, Report of the Steering Committee on Fintech Related Issues, (2019) available at: [https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech\\_1.pdf](https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech_1.pdf)

<sup>lxi</sup> See Financial Stability Board & Committee on the Global Financial System, FinTech credit: Market structure, business models and financial stability implications, (2017), available at: <https://www.fsb.org/wp-content/uploads/CGFS-FSB-Report-on-FinTech-Credit.pdf>

<sup>lxii</sup> See A. Tiwari, Challenges and future for India's neo-banks, Asia Business Law Journal, (2021), available at: <https://law.asia/challenges-future-india-neo-banks/>

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

<sup>lxiv</sup> Yan Carriere Swallow, Vikram Haksar and Manasa Patnam, India's approach to open banking: some implications for financial inclusion, International Monetary Fund, (2021), available at: <https://www.imf.org/en/Publications/WP/Issues/2021/02/26/Indias-Approach-to-Open-Banking-Some-Implications-for-Financial-Inclusion-50049>

<sup>lxv</sup> See Reserve Bank of India, Discussion Paper on "for-profit" Companies as Business Correspondents, (2010), available at: [https://www.rbi.org.in/scripts/bs\\_viewcontent.aspx?Id=2234](https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=2234)

<sup>lxvi</sup> See Reserve Bank of India, Discussion Paper on "for-profit" Companies as Business Correspondents, (2010), available at: [https://www.rbi.org.in/scripts/bs\\_viewcontent.aspx?Id=2234](https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=2234)

= <https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/>

<sup>lxviii</sup> Open Data Institute, Fingleton Associates, Data Sharing and Open Data for Banks - A report for HM Treasury and Cabinet Office, 16-17, (2014), available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/382273/141202\\_API\\_Report\\_FINAL.PDF](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF) (last accessed on May 25th, 2022).

<sup>lxix</sup> Open Data Institute, Fingleton Associates, Data Sharing and Open Data for Banks - A report for HM Treasury and Cabinet Office, 16-17, (2014), available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/382273/141202\\_API\\_Report\\_FINAL.PDF](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF) (last accessed on May 25th, 2022).

<sup>lxx</sup> Open Data Institute, Fingleton Associates, Data Sharing and Open Data for Banks - A report for HM Treasury and Cabinet Office, 16-17, (2014), available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/382273/141202\\_API\\_Report\\_FINAL.PDF](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF) (last accessed on May 25th, 2022).

<sup>lxxi</sup> See OECD, Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis, (2020) retrieved from <https://www.oecd.org/finance/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf>

<sup>lxxii</sup> See National Institute of Standards and Technology, NIST Big Data Interoperability Framework: Volume 1, Definitions, 12, (2015) available at: [https://bigdatawg.nist.gov/\\_uploadfiles/NIST.SP.1500-1.pdf](https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf)

<sup>lxxiii</sup> See Punjab National Bank v. Rupa Mahajan Pahwa, 2015 SCC Online NCDRC 3008.

<sup>lxxiv</sup> For more on the methodology of customer journey mapping as applied to the insurance sector, see A. Koning and G. Murthy, Customer Empowerment in Finance, Consultative Group to Assist the Poor (CGAP), Perspectives No. 3, August 2017 available at [https://www.cgap.org/sites/default/files/researches/documents/Perspective-Customer-Empowerment-in-Finance-Aug-2017\\_0.pdf](https://www.cgap.org/sites/default/files/researches/documents/Perspective-Customer-Empowerment-in-Finance-Aug-2017_0.pdf) (last accessed on October 22, 2021).

<sup>lxxv</sup> Dvara Research, Insights from the "Digital Credit Roundtable" hosted by the Future of Finance Initiative, 03 July 2017, available at <https://www.dvara.com/research/blog/2017/07/03/insights-from-the-digital-credit-roundtable-hosted-by-the-future-of-finance-initiative/>; Tiwari, S., Sharma, S., Shetty, S. and Packer, F., The design of a data governance system, BANK FOR INTERNATIONAL SETTLEMENTS, May 2022, available at <https://www.bis.org/publ/bppdf/bispap124.pdf>; Raghavan, M. and Singh, A., Building safe consumer data infrastructure in India: Account Aggregators in the financial sector (Part-2), DVARA RESEARCH, 07 January 2020, <https://www.dvara.com/research/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/>; Razis, G. and Mitropoulos, S., An integrated approach for the banking intranet/extranet information systems: the interoperability case, INTERNATIONAL JOURNAL OF BUSINESS AND SYSTEMS RESEARCH, retrieved from [https://www.researchgate.net/publication/341152094\\_An\\_integrated\\_approach\\_for\\_the\\_banking\\_intranetextranet\\_information\\_systems\\_the\\_interoperability\\_case](https://www.researchgate.net/publication/341152094_An_integrated_approach_for_the_banking_intranetextranet_information_systems_the_interoperability_case).

<sup>lxxvi</sup> See RBI, Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016.

<sup>lxxvii</sup> Originators can be understood as entities engaging in the design and delivery of financial services. These entities may be doing so directly or on behalf of banks or other regulated financial entities. See Dvara Research, IFMR Financial Systems Design Conference 2011 – Origination, 07 October 2011, available at <https://www.dvara.com/research/blog/2011/10/07/ifmr-financial-systems-design-conference-2011-origination/>.

<sup>lxxviii</sup> Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, BANK FOR INTERNATIONAL SETTLEMENTS, November 2019, available at <https://www.bis.org/bcbs/publ/d486.pdf>; Rathi, A. and Mohandas, S., FinTech in India: A study of privacy and security commitments, THE CENTRE FOR INTERNET AND SOCIETY, April 2019, available at <https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf>.

<sup>lxxix</sup> See Rule 3(ii), SPDI Rules.

<sup>lxxx</sup> See Tournier v. National Provincial and Union Bank of England, (1924) 1 KB 461 as discussed in Sengupta, 2021.



<sup>booxi</sup> See *Distt. Registrar v. Canara Bank*, (2005) 1 SCC 496.

<sup>booxii</sup> See Section 44, the State Bank of India Act of 1955.

<sup>booxiii</sup> See Section 25, the Regional Rural Banks Act of 1976.

<sup>booxiv</sup> See Section 13, the Banking Companies (Acquisition and Transfer of Undertakings) Act of 1980.

<sup>booxv</sup> See Sections 19 and 20, CIRC Act.

<sup>booxvi</sup> See Section 45E, the RBI Act.

<sup>booxvii</sup> See Section 22, PSSA.

<sup>booxviii</sup> See Reserve Bank of India, Notification on Storage of Payment System Data, (2018), retrieved from: <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0>

<sup>booxix</sup> Insolvency and Bankruptcy Board of India, Insolvency and Bankruptcy Board Of India (Information Utilities) Regulations, (2017), [https://ibbi.gov.in/uploads/legalframework/IU\\_Regulations\\_updated\\_till\\_25.07.2019.pdf](https://ibbi.gov.in/uploads/legalframework/IU_Regulations_updated_till_25.07.2019.pdf)

<sup>xc</sup> Reserve Bank of India, Master Direction on Digital Payment Security Controls, (2021), <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF>

<sup>xc<sup>i</sup></sup> See Reserve Bank of India, Master Direction on Know Your Customer Directions, 2016, (May 2021), [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=11566](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566)

<sup>xc<sup>ii</sup></sup> See Reserve Bank of India, Master Direction on Know Your Customer Directions, 2016, (May 2021), [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=11566](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566); RBI, Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions (2022), retrieved from: [https://rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=12300](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12300); RBI, Master Circular - Know Your Customer norms / Anti-Money Laundering Standards/ Combating of Financing of Terrorism /Obligation of banks under PMLA, 2002, (2008), retrieved from: [https://m.rbi.org.in/scripts/BS\\_ViewMasCirculardetails.aspx?Id=4354&Mode=0#int](https://m.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?Id=4354&Mode=0#int)

<sup>xc<sup>iii</sup></sup> See Reserve Bank of India, Master Circular on Credit Card, Debit Card, and Rupee Denominated Cobranded Prepaid Card Operations of Banks, (2014), [https://rbi.org.in/Scripts/BS\\_ViewMasCirculardetails.aspx?id=8998#6](https://rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=8998#6)

<sup>xc<sup>iv</sup></sup> See Reserve Bank of India, Circular on Storage of Payment System Data, (April 2018), <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244>

<sup>xc<sup>v</sup></sup> RBI, Master Directions on Account Aggregators (Reserve Bank) Directions, 2016 (as updated on December 29, 2022), retrieved from: [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=10598](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598)

<sup>xc<sup>vi</sup></sup> N. Dhavate, R. Mohapatra, A look at proposed changes to India's (Personal) Data Protection Bill, International Association of Privacy Professionals, (January 2022), <https://iapp.org/news/a/a-look-at-proposed-changes-to-indias-personal-data-protection-bill/>

<sup>xc<sup>vii</sup></sup> A. K. Joseph, India Can't Keep Delaying Its Personal Data Protection Bill, CARNEGIE INDIA, (April 2022), <https://carnegieindia.org/2022/04/14/india-can-t-keep-delaying-its-personal-data-protection-bill-pub-86885>

<sup>xc<sup>viii</sup></sup> A. Manikandan, Alternative data can gauge creditworthiness if law permits, ECONOMIC TIMES, (2019), <https://economictimes.indiatimes.com/markets/stocks/news/alternative-data-can-gauge-creditworthiness-if-law-permits/articleshow/68748552.cms>

<sup>xc<sup>ix</sup></sup> See *ICICI Bank Ltd. v. Umshankar Sivasubramanian*, 2019 SCC OnLine TDSAT 1561.

<sup>c</sup> A. Basu, Indian banks are using data from mobile bills and e-shopping to check customers' creditworthiness, SCROLL.IN, (April 2020), <https://scroll.in/article/959847/indian-banks-are-using-data-from-mobile-bills-and-e-shopping-to-check-customers-creditworthiness>

<sup>c<sup>i</sup></sup> R. Rao, Open Banking in India, (2021), <https://www.bis.org/review/r210419a.htm>

<sup>c<sup>ii</sup></sup> Dvara Research, Regulating data-driven finance: Conference proceedings, November 2020, <https://www.dvara.com/research/wp-content/uploads/2020/11/Conference-Proceedings-from-the-Fourth-Dvara-Research-Conference-2019.pdf>; Singh, A., Raghavan, M. and Chugh, B., Primer on Consumer Data Regulation, DVARA RESEARCH, 1 April 2019, <https://www.dvara.com/research/conference2019/wp-content/uploads/2019/04/Primer-on-Consumer-Data-Regulation.pdf>

<sup>c<sup>iii</sup></sup> Singh, A. and Prasad, S., Artificial Intelligence in Digital Credit in India, DVARA RESEARCH, 13 April 2020, <https://www.dvara.com/research/blog/2020/04/13/artificial-intelligence-in-digital-credit-in-india/>.

<sup>c<sup>iv</sup></sup> CGAP, Dalberg, and Dvara Research, "Privacy on the Line", Dvara Research, November 16, 2017, <https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>; Aditya Vashistha, Richard Anderson, and Shrirang Mare, "Examining the Use and Non-Use of Mobile Payment Systems for Merchant Payments in India," University of Washington, 2019, [https://ictd.cs.washington.edu/docs/papers/2019/vashistha\\_compass2019.pdf](https://ictd.cs.washington.edu/docs/papers/2019/vashistha_compass2019.pdf); Lakshay Narang, "Effects of Mobile-Based Financial Services on Migrant Households' Remittances and Savings," Dvara Research, August 24, 2020, <https://www.dvara.com/research/wp-content/uploads/2020/08/Effects-Of-Mobile-Based-Financial-Services-On-Migrant-Households-Remittances-And-Savings.pdf>; CGAP, Dalberg, and Dvara Research, "Privacy on the Line", Dvara Research, November 16, 2017, <https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>

<sup>c<sup>v</sup></sup> See European Commission, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, (2019), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN>

<sup>c<sup>vi</sup></sup> Prabhakkar, A., All about GDPR data segregation, INTERTRUST, 19 October 2021, available at <https://www.intertrust.com/blog/all-about-gdpr-data-segregation/> (accessed on 10 June 2022).

<sup>c<sup>vii</sup></sup> Notice is a key provision in the upcoming Digital Personal Data Protection Bill of 2022..

<sup>cviii</sup> DSCI, DSCI Privacy Framework: Best Practices, December 2010; Prabhakar, A., All about GDPR data segregation, INTERTRUST, 19 October 2021, available at <https://www.intertrust.com/blog/all-about-gdpr-data-segregation/> (accessed on 10 June 2022); Personal Data Protection Commission, Singapore, Trusted Data Sharing Framework, IMDA, 2019, retrieved from <https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf>.

<sup>cix</sup> Segregating personal data collected through two methods may have implications for when customers want to access their personal data records. Under the right to access, customers should ideally be receiving a break-up of information directly collected from customers and data obtained from third parties. Further, the purposes BSPs can use personal data collected from third parties could be different than data collected directly from customers.

<sup>cx</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Banking, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-banking-and-its-potential-impact-on-consumer-outcomes>; Kim, Y., Wang, Q and Roh, T., Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. 101483 Telematics and Informatics, (2020) retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0736585320301428>; Bleier, A., Goldfrab, A. & Tuckerc, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.

<sup>cx</sup> Susser, D., Notice After Notice-and-Consent: Why Privacy Disclosures are Valuable Even if Consent Frameworks Aren't, 9 Journal of Information Policy, 148-173 (2019); Kim, Y., Wang, Q and Roh, T., Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. 101483 Telematics and Informatics, (2020) retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0736585320301428>; Bleier, A., Goldfrab, A. & Tuckerc, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.

<sup>cxii</sup> Alliance for Financial Inclusion, Guideline note on data privacy for digital financial services, February 2021, retrieved from <https://www.sbs.gob.pe/Portals/0/jer/PUBLICACIONES/2021/Data-privacy-guideline-note.pdf>.

<sup>cxiii</sup> Notice is a key provision in the upcoming Digital Personal Data Protection Bill of 2022.

<sup>cxiv</sup> Tiwari, S., Sharma, S., Shetty, S. and Packer, F., The design of a data governance system, BANK FOR INTERNATIONAL SETTLEMENTS, May 2022, available at <https://www.bis.org/publ/bppdf/bispap124.pdf>.

<sup>cxv</sup> Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (February 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>.

<sup>cxvi</sup> Thompson, K. & Stockburger P., Data protection & consent: Comparing and contrasting changes to American and Canadian privacy laws, LEXPERT (May 2021), <https://www.lexpert.ca/legal-insights/data-protection-consent-comparing-and-contrasting-changes-to-american-and-canadian-privacy-laws/356250>.

<sup>cxvii</sup> The Personal Data Protection Bill, 2019, [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf); Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (2017), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; General Data Protection Regulation, Art. 13 GDPR Information to be provided where personal data are collected from the data subject, GDPR (2016), <https://gdpr-info.eu/art-13-gdpr/>; Personal Data Protection Act, 2012, <https://sso.agc.gov.sg/Act/PDPA2012?Provides=legis#legis>; DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxviii</sup> Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (February 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>.

<sup>cxix</sup> UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.

<sup>cxx</sup> The Personal Data Protection Bill, 2019, [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf); Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; General Data Protection Regulation, Art. 13 GDPR Information to be provided where personal data are collected from the data subject, GDPR (2016), <https://gdpr-info.eu/art-13-gdpr/>; Personal Data Protection Act, 2012, <https://sso.agc.gov.sg/Act/PDPA2012?Provides=legis#legis>; DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxxi</sup> Reserve Bank of India, Directions regarding Registration and Operations of NBFC – Account Aggregators under section 45-IA of the Reserve Bank of India Act, 1934, RESERVE BANK OF INDIA (2021) [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=3142](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142)

<sup>cxiii</sup> Calo, R., Against Notice Skepticism in Privacy (And Elsewhere), STANFORD CENTER FOR INTERNET AND SOCIETY (2011), <http://cyberlaw.stanford.edu/files/publication/files/ssrn-id1790144.pdf>; Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (February 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>; Solove, D.J., Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review, 1880 (2013), [https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty\\_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications); Gilbert, A., California Consumer Privacy Act (CCPA) compliance guide: Everything you need to know, OSANO (19 August 2021), <https://www.osano.com/articles/ccpa-guide>.

<sup>cxiii</sup> Fjeld, J. et.al, Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), <https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20>

White%20Paper%20Final\_v3.pdf?sequence=1&isAllowed=y; House of Commons Canada, Bill C-11, PARLIAMENT OF CANADA (November 2020), <https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading>.

<sup>xxxiv</sup> UK Information Commissioner's Office, Why is consent important?, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/why-is-consent-important/>.

<sup>xxxv</sup> Tiwari, S., Sharma, S., Shetty, S. and Packer, F., The design of a data governance system, BANK FOR INTERNATIONAL SETTLEMENTS, May 2022, available at <https://www.bis.org/publ/bppdf/bispap124.pdf>; UK Information Commissioner's Office, Why is consent important?, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/why-is-consent-important/>; CGAP, Dalberg & Dvara Research, Privacy on the Line: What people in India think about their data protection and privacy, DVARA RESEARCH (2017), <https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>; Bleier, A., Goldfrab, A. & Tuckerc, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.

<sup>xxxvi</sup> Notice is a key provision in the upcoming Digital Personal Data Protection Bill of 2022.

<sup>xxxvii</sup> Tiwari, S., Sharma, S., Shetty, S. and Packer, F., The design of a data governance system, BANK FOR INTERNATIONAL SETTLEMENTS, May 2022, available at <https://www.bis.org/publ/bppdf/bispap124.pdf>; Commonwealth of Australia, Open Banking: Customers, choice, convenience, confidence, AUSTRALIAN GOVERNMENT, December 2017, retrieved from [https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-\\_For-web-1.pdf](https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf).

<sup>xxxviii</sup> Reserve Bank of India, Directions regarding Registration and Operations of NBFC – Account Aggregators under section 45-IA of the Reserve Bank of India Act, 1934, RESERVE BANK OF INDIA (2021) [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?id=3142](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?id=3142); The Personal Data Protection Bill, 2019, clause 23(5), [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)

<sup>xxxix</sup> Tiwari, S., Sharma, S., Shetty, S. and Packer, F., The design of a data governance system, BANK FOR INTERNATIONAL SETTLEMENTS, May 2022, available at <https://www.bis.org/publ/bppdf/bispap124.pdf>.

<sup>xxxx</sup> Morey T., Forbath T., Schoop A., Customer Data: Designing for Transparency and Trust, Harvard Business Review (May 2015), <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>; Pacific Private Sector Development Initiative, Digital Financial Services in the Pacific: Experiences and Regulatory Issues, ASIAN DEVELOPMENT BANK (March 2016), <https://www.adb.org/publications/digital-financial-services-pacific>; Dvara Research, Dalberg & CGAP, Privacy on the Line: What people in India think about their data protection and privacy, DVARA RESEARCH (2017), <https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>.

<sup>xxxi</sup> Fjeld, J. et.al, Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), [https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final\\_v3.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y).

<sup>xxxii</sup> Office of the Privacy Commissioner of Canada, Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May 2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/); UK Information Commissioner's Office, Controllers checklist, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/controllers-checklist/>.

<sup>xxxiii</sup> UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.

<sup>xxxiv</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/healthcare-sector/>; Dvara Research, Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019, DVARA RESEARCH

(March 2020), <https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf>.

<sup>xxxv</sup> Dvara Research, Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019, DVARA RESEARCH (March 2020), <https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf>; UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.

<sup>xxxvi</sup> Tiwari, S., Sharma, S., Shetty, S. and Packer, F., The design of a data governance system, BANK FOR INTERNATIONAL SETTLEMENTS, May 2022, available at <https://www.bis.org/publ/bppdf/bispap124.pdf>; UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.

<sup>xxxvii</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Banking, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-banking-and-its-potential-impact-on-consumer-outcomes>.

<sup>xxxviii</sup> Ibid.

<sup>xxxix</sup> Data quality is a key provision in the upcoming Digital Personal Data Protection Bill of 2022.

<sup>cd</sup> The Personal Data Protection Bill, 2019, [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf); Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; General Data Protection Regulation, Art. 13 GDPR Information to be provided where personal data are collected from the data subject, GDPR (2016), <https://gdpr-info.eu/art-13-gdpr/>; Personal Data Protection Act, 2012, <https://sso.agc>.

gov.sg/Act/PDPA2012?ProvIds=legis#legis; DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxli</sup> Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 6 – Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accuracy/); The Royal Borough of Kensington and Chelsea, A Framework for better quality data and performance information, THE ROYAL BOROUGH OF KENSINGTON AND CHELSEA (2010), <https://www.rbkc.gov.uk/PDF/Data%20Quality%20Framework%20March%202010.pdf>.

<sup>cxlii</sup> OAIC, Chapter 10: APP 10 – Quality of personal information, OAIC (2019), <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information/>.

<sup>cxliii</sup> DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxliv</sup> Office on the Privacy Commissioner of Canada, Accuracy, OFFICE ON THE PRIVACY COMMISSIONER OF CANADA (2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/).

<sup>cxlv</sup> Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

<sup>cxlvi</sup> ISO, Data quality – Part 61: Data quality management: Process reference model, ISO (2016), <https://www.sis.se/api/document/preview/921215/>; Leo, L. et.al, Data Quality Assessment, 45 Communications of the ACM, 4 (2002), <http://web.mit.edu/tdqm/www/tdqmpub/PipinoLeeWangCACMApr02.pdf>; Batini, C. et.al, A Framework and a Methodology for Data Quality Assessment and Monitoring, MASSACHUSETTS INSTITUTE OF TECHNOLOGY (2007), <http://mitiq.mit.edu/iciq/pdf/a%20framework%20and%20a%20methodology%20for%20data%20quality%20assessment%20and%20monitoring.pdf>.

<sup>cxlvii</sup> DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxlviii</sup> UK Information Commissioner's Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>.

<sup>cxlix</sup> Ibid.

<sup>cl</sup> UK Information Commissioner's Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>; OAIC, Chapter 10: APP 10 – Quality of personal information, OAIC (2019), <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information/>.

<sup>cli</sup> Newsletter on cyber security, Bank for International Settlements, 20 September 2021, available at [https://www.bis.org/publ/bcbs\\_n125.htm](https://www.bis.org/publ/bcbs_n125.htm); OECD, Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data and privacy, 2020, retrieved from <https://www.oecd.org/finance/Financial-Consumer-Protection-Policy-Approaches-in-the-Digital-Age.pdf>.

<sup>clii</sup> Chen, S., D'Silva, D., Packer, F. and Tiwari, S., Virtual banking and beyond, BANK FOR INTERNATIONAL SETTLEMENTS, January 2022, available at <https://www.bis.org/publ/bppdf/bispap120.pdf>.

<sup>cliii</sup> Bank for International Settlements, Revisions to the Principles for the Sound Management of Operational Risk, March 2021, available at <https://www.bis.org/bcbs/publ/d515.pdf>.

<sup>cliv</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Banking, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-banking-and-its-potential-impact-on-consumer-outcomes>.

<sup>clv</sup> The obligation on providers to adopt security safeguards is a key provision in the upcoming Digital Personal Data Protection Bill of 2022.

<sup>clvi</sup> Alliance for Financial Inclusion, Policy model on consumer protection for digital financial services, 2020, available at [https://www.afi-global.org/sites/default/files/publications/2020-11/AFI\\_CEMC%2BDFS\\_PM\\_AW3\\_digital.pdf](https://www.afi-global.org/sites/default/files/publications/2020-11/AFI_CEMC%2BDFS_PM_AW3_digital.pdf); Monetary Authority of Singapore, Technology Risk Management Guidelines, January 2021, available at <https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf>; Digital Insight, Security controls and best practices for financial institutions, September 2015, [https://www.ncr.com/content/dam/ncrcom/content-type/datasheets/di\\_whitepaper\\_-\\_security\\_best\\_practices\\_0614.pdf](https://www.ncr.com/content/dam/ncrcom/content-type/datasheets/di_whitepaper_-_security_best_practices_0614.pdf); Commonwealth of Australia, Open Banking: Customers, choice, convenience, confidence, AUSTRALIAN GOVERNMENT, December 2017, retrieved from [https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking\\_-\\_For-web-1.pdf](https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking_-_For-web-1.pdf).

<sup>clvii</sup> Bank for International Settlements, Revisions to the Principles for the Sound Management of Operational Risk, March 2021, available at <https://www.bis.org/bcbs/publ/d515.pdf>.

<sup>clviii</sup> UK Information Commissioner's Office, Controllers checklist, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/controllers-checklist/>.

<sup>clix</sup> IRDAI, Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, 2017, <https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf>; Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 1 – Accountability, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (August 2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accountability/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/).



<sup>clx</sup> Data Protection Commission, Guidance Note: Guidance on Anonymisation and Pseudonymisation, DATA PROTECTION COMMISSION (June 2019), <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>.

<sup>clxi</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/healthcare-sector/>.

<sup>clxii</sup> PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>; Federal Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 5 – Limiting use, disclosure and retention, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_use/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/); MasterCard, The Global Data Responsibility Imperative, MASTERCARD (October 2019), <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf>.

<sup>clxiii</sup> Bank for International Settlements, Principles for Operational Resilience, March 2021, available at <https://www.bis.org/bcbs/publ/d516.pdf>; PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>; Federal Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); Personal Data Protection Commission, Guide to securing personal data in electronic medium, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2017), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/OtherGuides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf?la=en>; MasterCard, The Global Data Responsibility Imperative, MASTERCARD (October 2019), <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf>; National Standard of the People's Republic of China, Information security technology – Personal Information (PI) security specification, 2020, available at <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.

<sup>clxiv</sup> PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>; Federal Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); Federal Trade Commission, Start With Security, FEDERAL TRADE COMMISSION (2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>; MasterCard, The Global Data Responsibility Imperative, MASTERCARD (October 2019), <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf>.

<sup>clxv</sup> Federal Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>.

<sup>clxvi</sup> Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 7 – Safeguards, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_safeguards/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/).

<sup>clxvii</sup> PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>.

<sup>clxviii</sup> Personal Data Protection Commission, Guide To Securing Personal Data In Electronic Medium, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2015), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf?la=en>.

<sup>clxix</sup> Fjeld, J. et.al, Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), [https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final\\_v3.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y).

<sup>clxx</sup> UK Information Commissioner's Office, Security, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>; Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 5 – Limiting use, disclosure and retention, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_use/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/).

<sup>clxxi</sup> Bank for International Settlements, Revisions to the Principles for the Sound Management of Operational Risk, March 2021, available at <https://www.bis.org/bcbs/publ/d515.pdf>; IRDAI, Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, 2017, <https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf>; Dvara Research, The Dvara Data Protection Bill, 2018, DVARA RESEARCH (7 February 2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>.

<sup>i</sup> Privacy-by-design espouses seven foundational principles which guide providers in embedding privacy in the systems, standards, protocols and processes of providers. See, Information and Privacy Commissioner of Canada, Privacy and Security by Design, (2013) retrieved from: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf>

<sup>ii</sup> Security-by-design espouses principles for enabling and protecting data activities and assets against unauthorised access, use, disclosure, disruption, modification or destruction. The principles aim to maintain the integrity, confidentiality and availability of data. Ibid.

<sup>clxxii</sup> Cyber resilience good practices, Australian Securities and Investments Commission, 30 March 2021, available at <https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/>.

<sup>clxxiii</sup> Alliance for Financial Inclusion, Guideline note on data privacy for digital financial services, February 2021, retrieved from <https://www.sbs.gob.pe/Portals/0/jer/PUBLICACIONES/2021/Data-privacy-guideline-note.pdf>.

<sup>clxxiv</sup> Bank for International Settlements, Principles for Operational Resilience, March 2021, available at

<https://www.bis.org/bcbs/publ/d516.pdf>.

<sup>cbxxv</sup> Alliance for Financial Inclusion, Guideline note on data privacy for digital financial services, February 2021, retrieved from <https://www.sbs.gob.pe/Portals/0/jer/PUBLICACIONES/2021/Data-privacy-guideline-note.pdf>; Bank for International Settlements, Principles for Operational Resilience, March 2021, available at <https://www.bis.org/bcbs/publ/d516.pdf>.

<sup>cbxxvi</sup> Ibid.

<sup>cbxxvii</sup> Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (7 February 2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; National Standard of the People's Republic of China, Information security technology – Personal Information (PI) security specification, 2020, available at <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.

<sup>cbxxviii</sup> Hong Kong Monetary Authority, The Next Phase of the Banking Open API Journey, 2021, available at [https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The\\_Next\\_Phase\\_of\\_the\\_Banking\\_Open\\_API\\_Journey.pdf](https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The_Next_Phase_of_the_Banking_Open_API_Journey.pdf).

<sup>cbxxix</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, EUROPEAN COMMISSION, (2 April 2013), retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf).

<sup>cbxxx</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, EUROPEAN COMMISSION, (2 April 2013), retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf).

<sup>cbxxxi</sup> Consent is a key provision in the upcoming Digital Personal Data Protection Bill of 2022.

<sup>cbxxxii</sup> Reserve Bank of India, Master Directions on Credit Card and Debit – Issuance and Conduct, (2022), [https://rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=12300](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12300)

<sup>cbxxxiii</sup> Commonwealth of Australia, Open Banking: Customers, choice, convenience, confidence, AUSTRALIAN GOVERNMENT, December 2017, retrieved from [https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-\\_For-web-1.pdf](https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf).

<sup>cbxxxiv</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/healthcare-sector/>; Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>; GDPR, Article 14 - Information to be provided where personal data have not been obtained from the data subject, gdpr-info.eu: <https://gdpr-info.eu/art-14-gdpr/>.

<sup>cbxxxv</sup> National Standard of the People's Republic of China, Information security technology – Personal Information (PI) security specification, 2020, available at <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.

<sup>cbxxxvi</sup> Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorised Financial Data Sharing and Aggregation, 18 October 2017, available at [https://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

<sup>cbxxxvii</sup> Dvara Research, Dvara Data Protection Bill, 2018 - Cl.11(6), DVARA RESEARCH (7 February 2018) <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; UK Information Commissioner's Office, Right to data portability, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>; UK Information Commissioner's Office, Right to data portability, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>; Su, G., Singapore's PDPA's data portability obligation: Learning from the GDPR experience, WITHERS WORLDWIDE (3 February 2021), <https://www.withersworldwide.com/en-gb/insight/singapore-s-pdpa-s-data-portability-obligation-learning-from-the-gdpr-experience>; Su, G., Singapore's PDPA's data portability obligation: Learning from the GDPR experience, WITHERS WORLDWIDE (3 February 2021), <https://www.withersworldwide.com/en-gb/insight/singapore-s-pdpa-s-data-portability-obligation-learning-from-the-gdpr-experience>.

<sup>cbxxxviii</sup> Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorised Financial Data Sharing and Aggregation, 18 October 2017, available at [https://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

<sup>cbxxxix</sup> Reserve Bank of India, Directions regarding Registration and Operations of NBFC – Account Aggregators under section 45-IA of the Reserve Bank of India Act, 1934, RESERVE BANK OF INDIA (2021) [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?id=3142](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?id=3142); Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorised Financial Data Sharing and Aggregation, 18 October 2017, available at [https://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

<sup>cx</sup> UK Information Commissioner's Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>.

<sup>cxci</sup> Bleier, A., Goldfrab, A. & Tuckerc, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.

<sup>cxcii</sup> Kim, Y., Wang, Q and Roh, T., Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. 101483 Telematics and Informatics, (2020) retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0736585320301428>; Bleier, A., Goldfrab, A. & Tuckerc, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.

<sup>cxiii</sup> The right to confirmation, access, correction, and erasure are key provisions in the upcoming Digital Personal Data Protection Bill of 2022.

<sup>cxiv</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/>

healthcare-sector/; The Personal Data Protection Bill, 2019, clauses 18, 19 and 21, [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf).

<sup>ccv</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>ccvi</sup> DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>ccvii</sup> Office of the Privacy Commissioner of Canada, Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May 2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/).

<sup>ccviii</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>ccix</sup> Office of the Privacy Commissioner of Canada, Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May 2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/).

<sup>cc</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>cci</sup> The Personal Data Protection Bill, 2019, clause 17, [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)

<sup>ccii</sup> GDPR, Right of Access, <https://gdpr-info.eu/issues/right-of-access/>

<sup>cciii</sup> GDPR, Right of Access, <https://gdpr-info.eu/issues/right-of-access/>.

<sup>cciv</sup> Dvara Research, The Dvara Data Protection Bill, 2018, DVARA RESEARCH (7 February 2018), Retrieved from <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>.

<sup>ccv</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>ccvi</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Banking, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-banking-and-its-potential-impact-on-consumer-outcomes>; IAIS, Issues Paper on Increasing Digitalisation in Banking and its Potential Impact on Consumer Outcomes, IAIS (November 2018), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-banking-and-its-potential-impact-on-consumer-outcomes>.

<sup>ccvii</sup> See Digital Lending Report at page 12.

<sup>ccviii</sup> Fjeld, J. et.al., Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), [https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final\\_v3.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y).

<sup>ccix</sup> <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf>

<sup>ccx</sup> Superintendency of Industry and Commerce, Colombia, Sandbox on Privacy by Design and Default in AI, OECD (2020), <https://stip.oecd.org/stip/policy-initiatives/2019%2Fdata%2FpolicyInitiatives%2F26973>; Norwegian Data Protection Authority, Framework for the Regulatory Sandbox, DATATILSYNET (13 January 2021), <https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/framework-for-the-regulatory-sandbox/?print=true>; Global Privacy Assembly, Adopted Resolution on Accountability in the Development and Use of Artificial Intelligence, GLOBAL PRIVACY ASSEMBLY (2020), <https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN-1.pdf>; European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, EUROPEAN COMMISSION (2020), [https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf); High-level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, EUROPEAN COMMISSION (April 8 2019), retrieved from European Commission: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>; Dvara Research, Response dated 15 January 2021 to the Working Document: Enforcement Mechanisms for Responsible AI for All released by the NITI Aayog in November 2020, DVARA RESEARCH (18 January 2021), <https://www.dvara.com/research/wp-content/uploads/2021/01/Our-Response-to-the-Working-Document-on-Enforcement-Mechanisms-for-Responsible-AI-for-All.pdf>.

<sup>ccxi</sup> <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf>

<sup>ccxii</sup> The Government of Canada, Directive on Automated Decision Making, THE GOVERNMENT OF CANADA (5 February 2019), <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

<sup>ccxiii</sup> UK Information Commissioner's Office, Rights related to automated decision making including profiling, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>; General Data Protection Regulation, 2016, art. 22, <https://gdpr-info.eu/art-22-gdpr/>.

<sup>ccxiv</sup> Access Now, Human Rights in the Age of Artificial Intelligence, ACCESS NOW (November 2018), <https://www.accessnow.org/>

cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf; Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

<sup>ccxv</sup> Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

<sup>ccxvi</sup> Access Now, Human Rights in the Age of Artificial Intelligence, ACCESS NOW (November 2018), <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.

<sup>ccxvii</sup> Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

<sup>ccxviii</sup> Smart Dubai, Artificial Intelligence Principles and Ethics, SMART DUBAI (2019), <https://www.smartdubai.ae/initiatives/ai-ethics>.

<sup>ccxix</sup> OECD, The OECD Privacy Framework, OECD (2013), [https://www.oecd.org/digital/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/digital/ieconomy/oecd_privacy_framework.pdf); Robison, S.C., Trust, transparency, and

openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI), 63© Technology in Society, (2020), <https://ideas.repec.org/a/eee/teinso/v63y2020ics0160791x20303766.html>; Christina, H. & Dominik, E, Trust and privacy: How trust affects individuals' willingness to disclose personal information, IW-Report No 19/2018, (2018) <https://www.econstor.eu/bitstream/10419/179245/1/1023107090.pdf>.

<sup>ccxx</sup> Similar obligations may likely be introduced under the upcoming Digital Personal Data Protection Bill of 2022.

<sup>ccxxi</sup> Alliance for Financial Inclusion, Guideline note on data privacy for digital financial services, February 2021, retrieved from <https://www.sbs.gob.pe/Portals/0/jer/PUBLICACIONES/2021/Data-privacy-guideline-note.pdf>; Association of Banks in Singapore, Data sharing handbook for banks and non-bank data ecosystem partners, 30 August 2021, available at <https://abs.org.sg/docs/library/data-sharing-handbook-for-banks-and-non-bank-data-ecosystem-partners.pdf>; OECD, Financial consumer protection policy approaches in the digital age: Protecting consumers' assets, data and privacy, available at <https://www.oecd.org/finance/Financial-Consumer-Protection-Policy-Approaches-in-the-Digital-Age.pdf>.

<sup>ccxxii</sup> Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 1 – Accountability, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (August 2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accountability/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/); Alliance for Financial Inclusion, Guideline note on data privacy for digital financial services, February 2021, retrieved from <https://www.sbs.gob.pe/Portals/0/jer/PUBLICACIONES/2021/Data-privacy-guideline-note.pdf>.

<sup>ccxxiii</sup> Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 1 – Accountability, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (August 2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accountability/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/); DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>; Alliance for Financial Inclusion, Guideline note on data privacy for digital financial services, February 2021, retrieved from <https://www.sbs.gob.pe/Portals/0/jer/PUBLICACIONES/2021/Data-privacy-guideline-note.pdf>.

<sup>ccxxiv</sup> UK Information Commissioner's Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>.

<sup>ccxxv</sup> Ibid.

<sup>ccxxvi</sup> IRDAI, Guidelines of Banking E-commerce, rule 14(a), retrieved from [https://www.irdai.gov.in/admincms/cms/frmGeneral\\_Layout.aspx?page=PageNo3089&flag=1](https://www.irdai.gov.in/admincms/cms/frmGeneral_Layout.aspx?page=PageNo3089&flag=1).

<sup>ccxxvii</sup> Alliance for Financial Inclusion, Guideline note on data privacy for digital financial services, February 2021, retrieved from <https://www.sbs.gob.pe/Portals/0/jer/PUBLICACIONES/2021/Data-privacy-guideline-note.pdf>.

<sup>ccxxviii</sup> International Telecommunications Union, GSR 2019 Discussion Paper: Building confidence in a data driven economy by assuring consumer redress, INTERNATIONAL TELECOMMUNICATIONS UNION (2019), [https://www.itu.int/en/ITU-D/Conferences/GSR/2019/Documents/Consumer-Redress-digital-economy\\_GSR19.pdf](https://www.itu.int/en/ITU-D/Conferences/GSR/2019/Documents/Consumer-Redress-digital-economy_GSR19.pdf); UN Conference for Trade and Development, Manual on Consumer Protection, UNCTAD, UNCTAD (2016), <https://unctad.org/en/PublicationsLibrary/webditcclp2016d1.pdf>; Task Force on Financial Redress Agency, Report of the Task Force on Financial Redress Agency, DEPARTMENT OF ECONOMIC AFFAIRS (June 2016), [https://dea.gov.in/sites/default/files/Report\\_TaskForce\\_FRA\\_26122016.pdf](https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf); Financial Sectors Legislative Reforms Commission, Report of the Financial Sectors Legislative Reforms Commission, DEPARTMENT OF ECONOMIC AFFAIRS (March, 2013), [https://dea.gov.in/sites/default/files/fslrc\\_report\\_vol1\\_1.pdf](https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf); Indian Institute of Public Administration, Public Grievance Redress and Monitoring System in Government of India Ministries and Departments, DEPARTMENT OF ADMINISTRATIVE REFORMS AND PUBLIC GRIEVANCES (2008), [https://darpg.gov.in/sites/default/files/IIPA\\_Report\\_GRM.pdf](https://darpg.gov.in/sites/default/files/IIPA_Report_GRM.pdf); Kinhal, D., et.al., ODR: The Future of DBSPute Resolution in India, VIDHI CENTRE FOR LEGAL POLICY (July 2020), [https://vidhilegalpolicy.in/wp-content/uploads/2020/07/200727\\_ODR-The-future-of-dBSPute-resolution-in-India.pdf](https://vidhilegalpolicy.in/wp-content/uploads/2020/07/200727_ODR-The-future-of-dBSPute-resolution-in-India.pdf).



## Acknowledgement

---

On behalf of DSCI, we would like to extend our heartfelt gratitude to all the organizations and individuals for their valuable time and support, without which this guide would not have been possible. This guide is the result of directions and expert inputs of our esteemed advisory group, which included Ms. Shilpa Kumar, Partner at Omidyar Network India, and Mr. Rahul Rajendraprasad, Deputy Vice President and Data Privacy Officer at HDFC Bank Limited.

We would also like to thank Omidyar Network India for their support.

## About DSCI

---

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. For more information, visit: **[www.dsci.in](http://www.dsci.in)**

## Research Partner

---

Dvara Research is a policy research institution based in India. We are a not-for-profit, non-revenue generating policy think tank. Dvara Research's mission is to ensure that every individual and every enterprise has complete access to financial services. Dvara Research strongly believes in the deeply transformative power of finance in unlocking the potential of individuals, households, enterprises and local governments.

## Supported By

---

Omidyar Network India (ONI) invests in bold entrepreneurs who help create a meaningful life for every Indian, especially the hundreds of millions of Indians in low-income and lower-middle-income populations, ranging from the poorest among us to the existing middle class. To drive empowerment and impact at scale, ONI works with entrepreneurs in the private, non-profit and public sectors, who are tackling India's hardest and most chronic problems.

Omidyar Network India invests in the areas of Advancing Cities, Digital Society, Education & Employability, Emerging Technologies, Financial Inclusion & Well-being, and Property Inclusivity.

**For more information, visit: [www.omidyarnetwork.in](http://www.omidyarnetwork.in)**

## Notes

Notes

Lined area for notes.



## DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 4th Floor, Plot.No.7-10, Sector 126, Noida, UP - 201303

For any queries, contact:

P:+91-120-4990253 | E:info@dsci.in | W: www.dsci.in



DSCI\_Connect



dsci.connect



dsci.connect



data-security-council-of-india



dscivideo