Digital Personal Data Protection Policy

Indian Bank's Digital Personal Data Protection Policy envisages sound principles of Customer privacy and provides for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes. This policy may also be referred as Privacy Policy. The Bank is committed to the highest degree of Privacy Promise for its Customers and other stakeholders.

Indian Bank Privacy Promise for Customers:

While information is the cornerstone of the Bank's ability to provide superior service and customer satisfaction, one of the most important asset of the Bank is the customer's trust. Keeping customer information secure and using it only in the manner and for the specific purpose the customers would want the Bank to, is a top priority for everyone in the Bank. This becomes the Bank's promise to its customers and other stakeholders.

This policy governs the way in which the Bank collects, uses, processes, discloses, stores, secures and disposes of personal information and sensitive personal data or information of customer. The content present in this policy is subject to compliance with all the applicable laws, associated regulations and RBI guidelines.

Unless the context otherwise requires in this policy, reference to one gender includes a reference to the other, words importing the singular include the plural and words denoting natural persons include artificial legal persons and vice versa.

What Data the Bank collects?

1) Bank collects permitted personal, financial and marketing data to receive, possess, store, use, deal, handle, transfer, and otherwise process as per applicable laws.

    a. Personal data: This includes name, address, email addresses, phone/mobile number, KYC/identity documents (for example: Aadhaar and PAN), biometric data, device and location data, etc of the customer.
    b. Financial data: This includes information about customer's Bank account details, financial information, payment credentials, transaction data, loan details such as amounts and repayments, credit history and income details.
    c. Marketing data: This includes customer preferences relating to receiving marketing messages from Bank and its service providers, and customer communication preferences.

2) Any person giving aforesaid information to the Bank for any specific purpose shall deem to have given his consent for use, possess, store, deal, handle, transfer the same for that purpose and which may also be used to offer services for better customer experience. The information provided by a customer for a particular product/ services may also be used for

other product/ service offered by the Bank. Such person to note that the above Information/data provided to the Bank through any channel is true and accurate and he undertakes to ensure the accuracy and completeness of all Information/data disclosed, shared, exchanged. The person further undertakes to update and notify the Bank of any changes in the Information/data already provided to the Bank.

3) Customer may choose not to share personal data or withdraw consent, but doing so may limit the services which Bank is able to provide. However, customers shall not be able to withdraw any such data/ information which are mandatorily required to be obtained by the Bank under any Statutory/ Regulatory prescriptions.

How do the Bank collects customer data?

4) The Bank uses different methods and modes to collect Customer Information to provide services through Direct interactions, online applications, surveys, telephone conversations with Bank's call centres and any other communications as permitted by the Law and regulatory guidelines.

Purpose of collecting data:

5) The Bank or its service providers/contractors may hold and process customer's personal information on computer or otherwise in connection with Digital Lending or other activities through
Bank's Website, Internet banking, Mobile Banking, Kiosks, Tab Banking, branches and SMS(USSD) Services to provide the customer with the best possible services/products using the customer data for Business rule engine decision making by statistical analysis, credit scoring etc.

6) Bank will limit the collection and use of customer information to the minimum required, delivering effective service to the customers, to administer Bank's business and to advise customers about the Bank's products, services and other safeguards.

7) Bank analyses customer's personal information in relation to Bank's products and services including applications, credit decisions, determining the eligibility for the products or services. The process may involve automated profiling and decision making, which means that Bank may process the personal data using software that is able to evaluate personal aspects and predict risks or outcomes.

Who do the Bank share customer data with?

8) Customer's data will be collected and used only with the consent of that customer. Customer will have the option to revoke the consent. However, it may limit the services which the Bank is able to provide. However, customers shall not be able to revoke any such consent which is mandatorily required to be obtained by the Bank under any Statutory/ Regulatory prescription.

9) The Bank will not reveal customer information to any external organization unless the Bank has previously informed the customer in disclosures or agreements and has been authorised by the customer OR as required by the law and statutory/ regulatory authorities.

10) Whenever the Bank hires other organizations to provide support services, the Bank will require them to conform to the Bank's privacy policy standards.

11) For purposes of credit reporting, recovery of dues, risk management, verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences, or where disclosure is necessary for compliance of a legal obligation, the Bank may exchange information about the customers with government agencies, statutory agencies as mandated under the law.

Retention of customer data:

12) The Bank keeps the personal data collected about the customer on our systems or with third parties for as long as required for the purpose for which it is obtained or even beyond the expiry of transactional or account based relationship with customer: (a) as required to comply with any legal and regulatory obligations to which we are subject or (b) for establishment, exercise or defence of legal claims.

Third party Links:

13) Bank's website, mobile banking application and Internet banking platform may contain links to external Govt. and private organizations for facilitating customer transactions and lending business. While such links are provided for customer convenience and as per regulatory guidelines, customer should be aware that accessing such links is at their own risk since these websites may have their own privacy policies and that we do not accept any responsibility or liability for any such links. The Bank cannot provide assurance as to the information handling practices of the linked websites. Further, the Bank is not responsible for any such personal data breaches of customer occurred due to sharing of their information including security credentials like login id, password, OTP etc. to any other person or on any other malicious/ fraudulent website/ application or due to any such reason.

Security:

14) Bank will safeguard, securely and confidentially, any information that the customers share with the Bank. The Bank will continue to maintain its tradition of not sharing the transaction information in customers' account with anyone except when required by law or statutory/ regulatory agencies.

15) Bank will give access to customer information to only those employees who are authorized to handle the customer information. Employees who violate Bank's Privacy Promise will be subject to the Bank's normal disciplinary process.

16) Bank and the LSPs (Lending Service Provider) engaged by the Bank comply with various technology standards, requirements on cybersecurity, guidelines on outsourcing of IT services stipulated by RBI and other agencies, or as may be specified from time to time, for undertaking digital lending.

Social Media:

17) Bank provide various functionalities such as digital on-boarding of customers through multiple digital channels like Bank's Website, Internet Banking, Mobile Banking, Assisted digital banking through Tab Banking/ Feet-on-Street, Digital Banking Units(DBUs), Self-service kiosks or through any other upcoming digital channels. The products / services thus offered will be guided through applicable policies / guidelines of the Bank.

a. Policy on Digital Banking Products and Services,
b. Deposits Policy
c. Know Your Customer (KYC) / Anti Money Laundering (AML) / Combating Financing of Terrorism(CFT) Policy of the Bank
d. Digital Payment Security Policy, SOP on Digital Payment Security Controls and Digital lending policy -RBI

Due diligence:

18) Bank will exercise due diligence about ensuring the accuracy of the information collected.

19) Bank may also carry out automated anti-money laundering and sanction checks. This means that Bank may automatically decide that customer pose a fraud or money laundering risk if the processing reveals customers' behaviour to be consistent with money laundering or known fraudulent conduct, is inconsistent with previous submissions, or appear to have deliberately hidden the true identity. Bank will report all such data/information breaches to Statutory/ Regulatory authority as prescribed under Law.

20) Bank may record and monitor the communications with the customer for security purposes.

Data Destruction:

21) Considering the time validity of the stored data, a data destruction process will be implemented. Depending on the criticality and relevance of data, storage data and media will be destroyed periodically in order to avoid misuse and the chance of obsolete data getting loaded erroneously in the system after the prescribed storage period. When information is available in other forms or can be extracted through other means, such Obsolete and non-critical data available in backup tapes become redundant. Such data backup beyond a period of one year can be destroyed after confirming that adequate backup in other forms are available and the external media / storage can be reused with proper formatting procedures.

22) When destroying such obsolete and non-critical data and media, proper records will be maintained about the media and data and mode of destruction. Proper procedures will be established to ensure that the data and media are totally destroyed giving no room for recovery. Methods like degaussing the data and destruction of media through thermal or chemical means should be used.
23) A data destruction log will be maintained with details of the activity. If this activity is outsourced to a third party, bank will obtain a data destruction certificate from the vendor that the data was successfully erased and is unrecoverable.

Grievance Redressal Mechanism

21. The Bank has appointed a Nodal Grievance Redressal Officer for resolution of all grievances of customers pertaining to digital personal data protection. The details are as under:

Name- Shri Amit Chaudhari

Designation: General Manager [KYC/AML]

Address: Indian Bank, Head Office, No.66 Rajaji Salai, Chennai –600001

Email: nodalofficer[at]indianbank[dot]co[dot]in

https://indianbank.in/departments/nodal-officers-banking-ombudsman-scheme-2016/

The Bank will continuously assess to ensure that customer privacy is respected and will conduct the business in a manner that fulfils the Bank's Promise. All materials published by the Indian Bank are protected and owned or controlled by Indian Bank or the party credited as the provider of the content.