Cover page

Policy Guide on Privacy in Banking in India

I. Review of Relevant Existing Legislation and Policies

The collection and processing of personal information by Banks in India is regulated by the laws and regulations promulgated by the legislature and the government, and the rules notified by the Reserve Bank of India. Along with these, the Banks are also bound by their own rules and policies, and the standards they choose to subscribe to. The following are the most important rules, regulations, and policies in this regard.

1. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011[1]

Notified by the Central Government under Section 43A of the Information Technology Act, 2000 (hereinafter 'IT Act' or 'Act') read with Section 87 of the Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter 'Rules') are meant to provide basic guidelines that a body corporate or any person who works on their behalf must follow in order to protect the personal and the sensitive personal information of their customers.

These Rules differentiate between Personal Information and Sensitive Personal Information,[2] and only provide protection for the collection, retention, disclosure, and transfer of Sensitive Personal Information. Furthermore, the Rules require body corporate to establish 'reasonable security practices' for the protection of personal information. The Rules refer to ISO 27001 as an example[3] of such standards, which has led to banks relying on ISO 27001. Despite being a recommended standard by the Government, it has been found that the ISO 27001 is practically quite lacking.

2. Master Circular consolidating the Know Your Customer Norms, Anti-Money Laundering Standards, Combating Financial Terrorism and obligations of banks under Prevention of Money Laundering Act, 2002[4]

This Master Circular, notified on the RBI website, consolidates all the obligations of the Indian Banks with regard to their collection and processing of customer information under the Know Your Customer Norms (hereinafter 'KYC Norms'), Anti-Money Laundering Standards (hereinafter 'AML Standards'), Combating Financial Terrorism (hereinafter 'CFT') and obligations of banks under Prevention of Money Laundering Act, 2002 (hereinafter 'PMLA'). These standards require the banks to formulate a KYC Policy that incorporates the following key elements:[5]

1. Customer Acceptance Policy
2. Customer Identification Procedure
3. Monitoring of Transactions
4. Risk Management

Under these norms, banks are required to use strict standards for collecting the identification and address information of their customers, checking customers for possible associations with known offenders or with the "Sanctions Lists" provided to the Bank.[6] Furthermore, banks are required to regularly monitor the transactions of their customers so as to "*[understand] the normal and reasonable activity of the customer*" in order to easily identify unusual behaviour in their account.[7] In this respect, Banks are required to perform ongoing due diligence with respect to their business relationship with every client and examine each client's transactions closely to ensure that they are not outside the expected pattern, which has been developed by what the Bank already knows about the customer.[8] The norms also require banks to group customers according to the risk they present. The extent to which an account is monitored is determined by the category that it falls into.[9] The norms require banks to notify the relevant

---

1 *Available* at http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
2 Personal Information is defined under the Rules, § (1) (i), and Sensitive Personal Information is defined under the Rules, § 3.
3 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011 § 8 (2).
4 *Available at* http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8179.
5 *Id*, § 2.2.
6 *Id*, §§ 2.13 & 2.14 (iv).
7 *Id*, § 2.9.
8 *Id*, § 2.9 (c).
9 *Id.* § 2.3(c).

authorities along with the detailed particulars of the account in question if the person is suspected of supporting or being part of criminal activities, and further require banks to freeze the financial assets of a person in case he or she is confirmed to be an offender, without any prior notification.[10] These norms are extended to apply to instances of correspondent banking as well,[11] and to all transactions which the bank in question may be a part of for the purposes of wire transfers.[12] The norms also require the appointment of a Principal Officer to ensure the proper monitoring and reporting of transactions,[13] and the maintenance of certain types of transaction records by the banks.[14]

The KYC Policy as given in the Master Circular has many implications for user privacy , insofar as it mandates constant and continued monitoring of all the transactions of the customer,[15] and yet remains mostly silent on whether or not the customer should be notified of this crucial fact. It also mandates the collection and continued storage of this data for at least five years,[16] but does not speak of deletion or destruction of the collected information. Thus, as has been discussed in further detail later, the norms require the customers' actions to be closely noted and recorded, but do not provide enough safeguards to protect the customers' information. Though the reasons such powers have been given to banks, i.e. for prevention of money laundering and combating financial terrorism, justify the measures to some extent, the powers seem excessive to their purpose. Furthermore, the validity of the purpose does not justify or require weak or absent safeguards ensuring the security of the customers' personal information.

3. BCSBI's Code of Banks' Commitment to Customers[17]

The Code of Banks' Commitment to Customers (hereinafter 'Code of Conduct') is a voluntary code for banks, which sets the minimum standards of banking practices they must follow while dealing with individual customers.[18] Though this Code does not have the power of law, violations of the code can be brought to the Banking Standards and Standards Body of India (BCSBI), and the Banking Ombudsman. In case the complaint qualifies as an issue with the system itself, BCSBI then takes steps to amend the systems and procedures so that the complaint does not reoccur.[19] In case the complaint is made to the Banking Ombudsman, the Ombudsman will initially seek to settle the complaint through mediation or conciliation, failing which the Ombudsman will pass a final award that the complainant can chose to accept or reject.[20] If the complainant is dissatisfied with the Ombudsman's decision, he or she can approach the appellate authority, i.e. the Deputy Governor of RBI.[21]

The Code has a number of privacy related requirements. For example, the Code requires banks to treat customer's personal information collected by them as private and confidential,[22] and notify the customer in case there is a change in his or her bank's terms and conditions.[23] Furthermore, the Code lists the circumstances in which Banks can reveal customer information, requires them to explain to the customers the extent of their rights under the existing legal framework to access personal records bank holds about them, and prohibits the bank from using customer information for marketing purposes without permission. [24] Details about privacy and confidentiality of the customers' personal information with regard to Credit Reference Agencies (hereinafter 'CRAs') can also be found in the Code.[25] In this regard, banks are required to explain to their customers when they might share the information they have collected on their customers with CRA's,[26] and what types of credit checks they make with the CRAs regarding their customers.[27]Though banks are allowed to share information with CRAs, they must also provide the customer with a copy of the credit information report obtained from the CRA.[28] Finally, the Code holds banks responsible for cooperating as an industry to ensure a secure and reliable banking system,[29] asks the customers to keep the bank up to date in case there is a change in the information they have supplied to the banks,[30] and lists other general security measures.

---

10 *Id*, §§ 2.14 (iv) b & 2.14 (vi).
11 *Id*, § 2.16.
12 *Id*, § 2.18.
13 *Id*, § 2.19.
14 *Id*, § 2.20.
15 *Id*, § 2.9.
16 *Id*, § 2.20, (iii) (a).
17 BCSBI's Code of Banks' Commitment to Customers, *available at* https://www.sbp.co.in/PdfFiles/BCSBI.pdf.
18 *Id*, § 1. Introduction.
19 Background of the BCSBI, available at http://www.bcsbi.org.in/Abt_Background.html ("*BCSBI is not a forum for redressal of individual grievances. BCSBI, however, examines each compliant to identify any systemic issue that may exist and takes up the matter with the respective bank to ensure that systems and procedures are suitably amended so that such complaints do not recur.*")
20 Reserve Bank of India, *FAQs on the Banking Ombudsman Scheme, available at* http://www.rbi.org.in/scripts/FAQView.aspx?Id=24.
21 *Id*.
22 *Id*, § 2.1.5
23 *Id*, § 3.5.1
24 *Id*, § 5. (The "*exceptional cases*" in which information can will be shared are:
"*a. If we have to give the information by law*
b. If there is a duty towards the public to reveal the information
c. If our interests require us to give the information (for example, to prevent fraud) but we will not use this as a reason for giving information about you or your accounts [including your name and address] to anyone else, including other companies in our group, for marketing purposes.
d. If you ask us to reveal the information, or if we have your permission
e. If we are asked to give a banker's reference about you, we will need your written permission before we give it.
f. We, will explain to you the extent of your rights under the existing legal framework for accessing the personal records that we hold about you.
g. We will not use your personal information for marketing purposes by anyone including ourselves unless you specifically authorize us to do so."
25 *Id*, § 5.1
26 *Id*, § 5.1 (b) (In the specific case of information regarding personal debts, banks can share information with Credit reference agencies if:
"*I. [the customer has] fallen behind with [his or her] payments;*
II. The amount owed is not in dispute; and
II. [the customer has] not made proposals [the bank is] satisfied with for repaying [his or her] debt, following [the bank's] formal demand."
27 Credit rating agencies give the banks a collection of data about the customer or prospective customer in question, including their credit history, which the banks can use for various purposes. The checks are made on the basis of this Credit Reference Report. (*See* CRISIL, CRISIL Rating FAQs, *available at*: http://crisil.com/ratings/faqs.html). An example would be Credit Risk reporting, which are used to calculate the risk of a prospective customer being unable to repay a loan, and on the basis of that accept or reject the loan application, or change the interest rate being charged.
28 *Id*, §§ 5.1 (d) & (e).
29 *Id*, § 9.1.
30 *Id*, § 9.2.

II. International Practices

This part of the guide reviews existing legislations and practices in the US, Canada, Australia, and the EU which govern the security and confidentiality of customer information collected, held or processed by banking institutions. The following are the most relevant legislations and practices in their respective jurisdictions.

1. United States – Gramm-Leach-Bliley Act, Title V – Privacy

Title V (hereinafter 'Title') of the Gramm-Leach Bliley Act (hereinafter 'GLBA') is the main legislation that addresses privacy in the financial sector in the United States. The Act covers banks and the information they collect, under the term 'financial institutions' as used in Sec. 501. The Title governs non-public personal information,[31] excluding all information available in the public domain from its purview. It places an obligation on financial institutions to respect customer privacy, and to protect the security and confidentiality of customer non-public personal information. The Code also requires financial institutions to notify their customers before disclosing their information to non-affiliated third parties, allow them to opt-out of such disclosure, limits the use of collected information to that which has been notified to the customer, and specifically prohibits the use of non-public information for marketing or any other purposes without consent,[32] and requires the financial institution to disclose to the customers their privacy policy in detail, and follow up on this disclosure annually.[33] The Secretary of Treasury is given the authority to conduct external studies of the information sharing practices among financial institutions and their affiliates under Sec. 508,[34] and Sec. 521 prescribes the guidelines "Privacy Protection for Customer Information of Financial Institutions", in the context of fraudulent access.[35] Notably, while financial information is subject to the standards of the GLBA, other types of information are covered under different standards set by other legislations, such as the HIPPA which governs health information.[36]

2. Australia – Privacy Act, 1988

Information Privacy in Australia is governed by the Privacy Act, 1988. The Act defines two sets of privacy principles, the National Privacy Principles[37] and the Information Privacy Principles.[38] While the Information Privacy Principles are limited to the Public Sector Agencies, the National Privacy Principles govern organisations defined under Section 6C of the Privacy Act. These principles set out rules for the collection,[39] use and disclosure,[40] data quality,[41] security,[42] openness,[43] access and correction,[44] identifiers,[45] anonymity,[46] trans-border data flows,[47] and sensitive information.[48] In the Australian model, the choice of application of the principles is not dependent on the type of information, but rather the ownership of the organisation in question. Thus, financial information is treated to the same standard as other types of sensitive information, i.e. the National Privacy Principles in the case of private organisations. The 13 Australian Privacy Principles are scheduled to replace the National Privacy Principles for organisations from 12 March 2014.[49] The only exception is Credit Information, which is governed by Part IIIA of the Privacy Act, which sets out what information credit providers can report and to whom.[50]

Australian Banks can further choose to follow the Australian Bank Association's (hereinafter 'ABA') Privacy Policy[51] and Code of Banking Practice.[52] According to the Policy, in case the customer believes that the ABA or a member bank has breached its obligations under the Privacy Act, he or she can complain to ABA or the bank respectively.[53] In case the ABA or the bank fails to address the complaint, the customer can complain to the Federal Privacy Commissioner.[54] Thus, the Privacy Policy itself is not enforceable. In case there is a breach of the Code of Banking Practice, the customer can issue a complaint to the Code Compliance Monitoring Committee (hereinafter 'CCMC'), which is an independent compliance monitoring body, or in case he or she has suffered a loss and is not satisfied with the internal dispute resolution, he or she can issue a complaint to the Financial Ombudsman Service (hereinafter 'FOS'), which is the bank's external dispute resolution scheme.[55] In case of a confirmed breach, the CCMC is allowed to indicate in its website and reports the name of the bank along with the breach it is guilty of.[56] In case the complaint is made to the FOS, it will resolve the dispute by negotiation, conciliation, or a formal decision on the basis of the merits of the case.[57] The Institutions can also develop their own 'Privacy Code' and have them verified by the Information Commissioner under Part IIIAA of the Privacy Act.[58]

3. Canada – Personal Information Protection and Electronic Documents Act, 2000[59]

The main legislation addressing data privacy in Canada is the Personal Information Protection and Electronic Documents Act, 2000 (hereinafter 'PIPEDA'). This legislation governs the activities of all businesses and federally regulated industries in how they collect, use, disclose safeguard and provide access to their customers' personal information. An individual's financial information is covered under the general head of 'personal information' as defined under Sec. 2(1) read with 4. (1) of Part I of PIPEDA, and banks are included under 'organizations' as defined under Sec. 2 and used in Sec. 4.(1). No distinction has been made under the PIPEDA between types of information collected on the individual, except to the extent of exclusion of general information about an employee,[60] and the separate category of 'personal health information'.[61] Thus, the financial information of an individual is subject to the same standards as other forms of sensitive information.

Earlier, Canadian banks could subscribe to the Canadian Banking Association's Privacy Code,[62] which was, they say, regularly updated to meet the needs of the customers.[63] The values of this code have been carried over in the Privacy Act.[64] Some banks still display a Privacy Policy on their website, though, which seems to have the same essential principles as the Act.[65]

---

31 15 USC 6801 (§ 501. Protection of Non-public Personal Information).
32 *Id*, §§ 502 (a) to (d).
33 *Id*, § 503.
34 15 USC 6808.
35 15 USC 6821. (This section, which sets out the Privacy Protection for Customer Information of Financial Institutions guidelines, essentially prohibits obtaining customer information by using false pretences and solicitation of a third party to do the same. It also lists exceptions to this prohibition, those being - Law Enforcement Agencies; Financial Institutions which are testing their security procedures; investigating allegations of misconduct or negligence or recovering customer information falsely obtained by another person' Insurance Institutions investigating insurance fraud; information available as public information pursuant to securities laws; and, to Private Investigators or their employees from obtaining information to the extent it is reasonably necessary to collect child support.)
36 100 Stat. 1936.
37 Privacy Act, 1988, Schedule 3, *available at* http://www.comlaw.gov.au/Series/C2004A03712.
38 *Id*, Part III, Division 2.
39 *Id*, note 28, Schedule 3, 1.
40 *Id*, schedule 3, 2.
41 *Id*, schedule 3, 3.
42 *Id*, schedule 3, 4.
43 *Id*, schedule 3, 5.
44 *Id*, schedule 3, 6.
45 *Id*, schedule 3, 7.
46 *Id*, schedule 3, 8.
47 *Id*, schedule 3, 9.
48 *Id*, schedule 3, 10.
49 Office of the Australian Information Commissioner, *Summary and analysis of key differences for organisations*, http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/australian-privacy-principles-and-national-privacy-principles-comparison-guide; a comparison guide between the National Privacy Principles and the Australian Privacy Principles is available at http://www.oaic.gov.au/images/documents/privacy/privacy-guides/comparison_guide_APP_NPP.pdf.
50 Privacy Act, *supra* note 36, Part IIIA – Credit Reporting.
51 *Available at* http://www.bankers.asn.au/Privacy-Policy.
52 *Available at* CCMC Mandate 2013 http://www.bankers.asn.au/Industry-Standards/ABAs-Code-of-Banking-Practice.
53 Australian Banks Association Privacy Policy, *supra* note 48, § 9.
54 *Id*.
55 Code of Banking Practice FAQs, *How can I enforce my rights under the Code?*, *available at* http://www.bankers.asn.au/ArticleDocuments/172/Code%20of%20Banking%20Practice%20FAQs.pdf.aspx.
56 The CCMC Mandate, Part F, § 36, (j), available at http://www.bankers.asn.au/ArticleDocuments/172/ABA_CODE_MANDATE_FINAL_LR.PDF.aspx. (" *to empower the CCMC to name [the bank] on the CCMC's website, in the next CCMC annual report, or both, in connection with a breach of this Code, where it can be shown that [the bank has]: i. been guilty of serious or systemic non-compliance; ii. ignored the CCMC's request to remedy a breach or failed to do so within a reasonable time; iii. breached an undertaking given to the CCMC; or iv. not taken steps to prevent a breach reoccurring after having been warned that [the bank] might be named.*")
57 Financial Ombudsman Service, *Dispute Handling Process in Detail*, *available at* http://www.fos.org.au/utils/pdf.jsp?id=1795&usepage=true.
58 Privacy Act, *supra* note 36, § 18BA.
59 Personal Information Protection and Electronic Documents Act, 2000, *available at* http://www.priv.gc.ca/leg_c/r_o_p_e.asp.
60 *Id*, Part I, Section 2.
61 *Id*, Part I, Section 2.
62 *Available at* http://www.cba.ca/en/consumer-information/43-rights-responsibilities/66-banks-and-your-privacy.
63 *Id*.
64 *Id.*
65 *See* the Bank of Canada Privacy Policy, *available at* http://www.bankofcanada.ca/privacy-statement/.

4. European Union – the Data Protection Directive, 95/46/EC

The most important source of law in the European Union (hereinafter 'EU') with respect to Data Privacy is the Data Protection Directive (hereinafter 'Directive').[66] It is a broad directive which covers all forms of personal data collection and processing, and mandates that such collection or processing follow the Data Protection Principles it sets out.[67] The Directive differentiates between Personal Data and Sensitive Personal Data,[68] with the collection and processing of the latter being subject to more stringent rules. The definition of Sensitive Personal Data under the EU Directive does not include financial data, thus making it simply personal data, but some member States have extended the definition to include data about debt, financial standing etc.. The Directive essentially restricts all forms of data processing unless the processing meets one or more of the following conditions: the data subject[69] consents to the processing, the processing is necessary under a contract the subject has agreed to, it is necessary for a legal obligation on the controller,[70] it is necessary to protect the vital interests of the data subject, it is necessary for a task carried out in public interest or in exercise of official authority vested in controller, or where it is necessary for legitimate interests of the controller or the third party to which the data is disclosed unless it violates the subject's fundamental rights or freedoms under the Directive.[71] The data subject must be notified of the identity of the controller, the purposes of data collection, the recipients of collected data, the consequences or lack thereof of not providing data, and the existence of the right to access or rectify data concerning him or her, and any other information as is necessary,[72] even in case the information has not been provided by the data subject himself.[73] The Directive specifies other principles regarding the collection, such as Data Quality,[74] of which Accuracy[75] is a part.

There are no other privacy laws or principles related to financial information that apply to the EU as a whole, the only exception being the Professional Secrecy provision in Article 12 of the First Banking Directive, which only applies to employees of financial institutions with regards to the customer financial information they obtain in the course of their employment.[76] Banks in the EU as a whole do not seem to be adhering to any other guidelines, but the Privacy Laws of each State under EU can be different, as noted above.

66 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
67 *Id*, article 3.
68 *Id*, article 8.
69 As defined in the Directive. (*Id,* article 1 (a)).
70 As used in the Directive. (*Id,* article 1 (d)).
71 *Id*, article 7.
72 *Id*, article 10.
73 *Id*, article 11.
74 *Id*, article 6.
75 *Id*, article 6 (d).
76 First Council Directive of 12 Dec. 1977 on the Coordination of Laws, Regulations and Administrative Provisions to the taking up and pursuit of the Business of Credit Institutions (77/780/EEC), art. 12.

III. Analysis

1. Methodology

To gain a practical perspective on the existing banking practices and policies in India in this project, an empirical study of five separate and diverse banks has been conducted. The forms, policy documents, and other relevant and available documents of these banks have been analysed in this project. These documents were obtained from the websites of the respective banks, and wherever they were lacking, from the branches of the banks themselves. Attempts were made to obtain any information required for the project that was not available on the website or in the forms from the officers of the respective banks.

The State Banks of India (hereinafter 'SBI'), Central Bank of India (hereinafter 'CBI'), ICICI Bank (hereinafter 'ICICI'), IndusInd Bank (hereinafter 'IndusInd') and Standard Chartered Bank (hereinafter 'SCB') are the banks chosen for this project. As mentioned, these banks have been chosen to ensure a diverse sample pool. SBI is an Indian public multinational bank, CBI is an Indian public bank and it is not multinational, ICICI is an Indian private and multinational bank, IndusInd is an Indian private bank which isn't multinational, and SCB is a British bank operating in India.

The forms and other documents of each of the banks have been compared against a template of twenty nine questions created from the nine principles given in Justice A.P. Shah Group of Experts' Report on Privacy.[77] The two services provided by these banks that have been analysed are Opening an Account and Taking out a Personal Loan. This comparison has been done keeping in mind the obligations of the banks under the Master Circular and the KYC Norms detailed in it, Code of Conduct, and the Rules under Section 43A of the IT Act. Attempts have been made to clarify the basis of the response as much as possible. An analysis of the obligations of the banks is present below, along with an explanation of the relevance of various parts of the two services that are analysed.

2. Summary of Relevant Rules and Legislations

Under the KYC Norms, banks are obligated to collect and update the Name and Address information of their existing and new customers. At the same time, they must also monitor all the transactions of their customers and keep an eye for anomalies, and also create a profile of their general account behaviour to better point out unusual behaviour.[78] The Code of Conduct mandates that the banks who have subscribed to the Code inform their customers about the following:

1. The extent of the customer's rights to access the personal records held by the bank on him or her in the existing legal framework.[79]
2. Changes to Term and Conditions, presumably including the changes to the type and form of collection and processing of financial information.[80]

Furthermore, the banks are obligated to treat the customer's information as private and confidential,[81] and not share collected information unless it meets the criteria given in the Code of Conduct, with a specific section of the Code of Conduct being dedicated to Credit Reference Agencies.[82] Under the Code of Conduct, banks cannot use collected information for marketing purposes without the specific authorisation of the customer.[83] The Code also places on the banks the onus of "*[acting] as an industry*" to ensure a secure and reliable banking system for the customers.[84]

The Rules mandate that bodies corporate, which would here be the banks, follow 'Reasonable Security Practices', listing ISO 27001 as an example,[85] and that they have their Codes of Best Practice are duly approved and notified by the Central

77 *Available at* planningcommission.nic.in/reports/genrep/rep_privacy.pdf.
78 RBI Master Circular, *supra* note 4, as cited in *supra* note 15.
79 BCSBI, *supra* note 16, § 5 (f).
80 *Id*, § 3.5.
81 *Id*, § 5.
82 *Id*, § 5.1.
83 *Id*, § 5.g.
84 *Id*, § 5.9.1.
85 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules) Rules, *supra* note 3, §§ 8.1 & 8.2.

Government.[86] Most importantly, the Rules also mandate an audit of the reasonable security practices and procedures of the bodies corporate, which is to be conducted at least once a year or as and when the concerned institution undertakes significant upgradation of its process and computer resource.[87] The Rules also address the Collection[88] and Disclosure of Information,[89] along the same lines[90] as the terms given in the Code of Conduct, with the exception of the fact that the Rules also add the principles of Notification,[91] about the information that is collected and other related information, Retention,[92] Consent,[93] and Necessity.[94]

Thus, of the nine principles laid out in the Shah Committee Report,[95] the banks are essentially directly obligated to follow all except Openness. And even the principle of Openness is indirectly integrated into the other principles, as is clear from the questions in the template.

3. Observations

Before analysing the results of the study itself, some points observed during the research for this project must be noted. First and foremost, in all the branches that were visited, information about the topic of privacy from the officers of the bank was not easily obtainable. Furthermore, whatever information was available through forms and documents was scattered throughout various documents, such as Account Opening Forms or Loan Application Forms, KYC Policy documentation, Privacy Policy, and Most Important Terms and Conditions, some of which were not available online and had to be obtained from a branch of the bank in question. Thus, though some of the information related to privacy is presented clearly, it would take an inquisitive and educated customer to find out all the details of the rules applicable to his or her account, which in the experience of the banks is rarely the case.[96] Some of the banks claim that all the official documentation is given to the customer once they open an account in a 'Welcome Kit', but this essentially means that the information is given to the customer once he or she has already become a customer and shared his or her personal information. This also highlights the fact that customers only have a limited amount of choice when engaging with a financial institution, as is usually the case with Standard Form Contracts. If the customer does not like the terms and conditions offered by one bank, they can only choose to go to another bank, which may or may not actually make much of a difference. Thus, the lack of choice coupled with the lack of information and the lack of accessibility makes it difficult for customers to make informed decisions with respect to their personal information when engaging and transacting with a bank. This is particularly true for those who are unaware of the privacy concerns in the context of banking.

4. Results

The results of this study are visible in the attached Template. The main points from the study include:

1. The information provided by the banks to their customers regarding the security, collection and processing of their information is quite lacking, as the Template indicates. The customers are not provided sufficient details regarding the collection, processing, or security of their personal data. In most cases, they are not even given enough information about the legal framework surrounding the collection and processing of personal information. A very general statement regarding the fact that the bank may share information as and when necessary with whichever person is necessary to meet its obligations under various laws/regulations/standards is given in almost all the AOFs, and all of the loan application forms. The Code of Conduct mandates that the banks notify the customer about the legal framework governing the customer's access to collected information, but no such explanation is provided on the website or in the forms.[97]
2. The customer is allowed almost no choice with regards to the processing of his or her information. This is true especially with regard to third party processing of information, where the customer should ideally always be given the choice to not consent.
3. The deletion of the information is not mandated and is in all likelihood not carried out – anecdotal evidence offers that the information is just archived after the mandated retention period runs out.[98]
4. The onus of alerting the bank in case of change of any information is entirely on the customer.
5. There is no formal framework which allows the user to access the entirety of information collected on him or her.
6. The documents which detail information relevant to these concerns are not easy to obtain, or navigate, and is not nearly detailed enough.
7. Details on the audit mechanism could not be obtained from the banks, as it is a confidential bank policy. The presence or absence of an internal audit system has been noted in the Template on the basis of the response of the banks' officers to the question. No clarifications regarding external audits question were provided by the banks. They only explained their existing internal audit system again. Thus, for the purpose of the research, this question has been left unevaluated.
8. There is no bank officer specifically in charge of Privacy Concerns.

---

86 *Id*, § 8.3.
87 *Id*, § 8.4.
88 *Id*, § 5.
89 *Id*, § 6.
90 Both, the Code of Banks' Commitment to Customers and the Rules under 43A allow for Disclosure of Information only when it is necessary, or when the data subject has consented to it. Disclosure is considered necessary when it is legally required, or when it has been agreed to in the contract, and any third party receiving this information cannot disclose it further. The difference between the two is that the Rules specifically include an exception which obligates the banks to share personal information with Government agencies for the purpose of prevention, detection or investigation of offences, whereas the Code includes an exception which allows the banks to share the information if required by law as well as for their interests as long as it is not for marketing purposes, and another exception which allows banks to disclose personal information in case it is the banks duty to the public to do so. Though the Code does not address the Collection principle specifically, they indicate that a level of care must be taken in the collection of personal information. The Rules on the hand specifies that Sensitive Personal Data shall not be collected unless it is for a lawful activity of the body corporate or a person on its behalf.
91 *Id*, § 5. (3).
92 *Id*, § 5. (4).
93 *Id*, §§ 5. (1) & (7).
94 *Id*, § 5. (2).
95 Justice AP Shah Committee Report, s*upra* note 76, Ch. 3 (The principles mentioned in the report are: Openness, Accountability, Notice, Choice & Consent, Collection Limitation, Use Limitation, Access & Correction, Security, Disclosure & Third Party Use).
96 Based on responses of the bank officials to query.
97 BCSBI, *supra* note 16, § 5 (f).
98 Based on responses of the bank officials to questions in the Template.

IV. Conclusion and Recommendations

The main issues regarding the privacy of the customers that are highlighted by the results of the study and the recommendations for addressing them can be categorised as given below.

These recommendations are based off of the National Privacy Principles given in the Shah Committee Report:[99]

1. Customers are not given all the information that they ideally should, such as details of the types of information that are collected, details of information that is shared with third parties, and the security measures of the bank. The information that *is* available to the customers is scattered throughout various documents.[100]
2. The customers are usually not given the choice to not consent to or opt out of the processing of information for non-mandatory purposes.[101] Though the Code of Conduct mandates that personal information not be used for marketing purposes without the customer's consent, this consent, or more importantly the lack of one should be specified in the official documents.
   Recommendation: There should be one comprehensive document that addresses all of the customer's privacy concerns. Such a document would then include all the information the customer should have, specifically including what information is shared, with whom and why, should mention the customer's consent or the lack of it, and should be easy to understand. The banks should also create a formal framework which the customer can use to access his or her information, and notify their customers about the same. To facilitate legibility, this document should be available in the major languages of the region. This would help the banks with the Notification, Consent, Disclosure & Information and Openness principles.
3. The onus of gathering information and being aware of the privacy concerns is entirely on the customer. The bank has no obligation to make the customers aware about the collection and processing of their sensitive personal financial data.
   Recommendation: As an addition to the above recommendation, the onus of informing the customer about the privacy concerns they should have and clarifying all the details of the process should be on the banks, and not on the customers. Furthermore, it should be the banks' obligation to ensure that the information they have is up-to-date and accurate. This would help the banks with the Notification and Access and Correction principles.
4. The personal information collected by the banks is mandatorily retained for a fixed number of years,[102] but deletion of this information is not legally mandated. Thus, it is possibly archived by the banks, and deleted or retained as it suits them.
   Recommendation: Deletion of personal information as soon as it is no longer useful for the purpose that it has been collected for must be made legally mandatory. This would help the banks with the Deletion principle.
5. Though the customers are currently able to access the information collected by the banks on them, this access and its legal basis is not specifically mentioned in the documents given by the banks.
   Recommendation: The customer should at all times be able to access whatever information the bank has on him or her, as long as it does not violate a third person's privacy. This should be clearly mentioned in the documents in order to leave no doubt and to allow the customer to enforce this right in case of a dispute. This would help the banks with the Access and Correction principle.
6. Though there is a usually a Nodal Grievance Officer in place, this officer is to handle all the complaints that come through the complaint process. It is also not necessary that this officer is entirely familiar with the banks' policies regarding data security and privacy.
   Recommendation: There should be a separate officer who is specifically tasked with handling the privacy concerns of customers. Such an officer should know all the details of the data collection and processing in order to address any problems the customer might have, including the banks' audits. This would help the banks with the Accountability principle.

The following recommendations focus on the IT Act and the IT Rules, based on the opinions of individuals engaged in the field:

1. Though financial information has been included in the definition of 'sensitive personal information' or 'personal information' under the IT Rules, this definition is not well drafted, and leaves room for interpretation about its exact constituents. This should be changed so as to leave no doubt that it includes all personal information collected by the banks, thereby placing on them the onus of protecting the information they collect from their customers. Ideally speaking, these terms should be defined proactively in order to ensure them being relevant despite technological advancements.
2. The Burden of Proof for any cases under the IT Rules should be on the body corporate, as long as the data subject can prove that some personal information has been lost or misused.
3. The standard that the IT Rules specify is the ISO 27001, which has been noted for its weakness. It is essentially a simple checklist, and the banks do not even need to indicate how many standards on the checklist they meet. A different standard should be used as an example, which puts in place as many transparency measures as possible without damaging the security of the customer's information.
4. Rule 5(2) of the IT Rules should be amended to allow collection of personal information only when strictly necessary. In their current form, they allow for collection of information for any lawful purpose directly connected to the body corporate or a person acting on its behalf, which is too broad a field. It should be restricted in accordance with the Collection Principle as mentioned in the Shah Committee Report.[103]

[99] Annexure 1.

[100] For example, in the case of IndusInd, though the bank gives the customer a reasonable amount of information about the KYC Norms and their own KYC Policy, this is given in the KYC FAQ, which is given separately from the Account Opening Form, which barely addresses the KYC Norms or IndusInd's KYC Policy at all.

[101] Of the five banks, only one, ICICI, gave the customer the option of not consenting to having his or her information used for marketing purposes. Such an option was not given in the forms of the other banks. Though IndusInd has given its customers the option of withdrawing from being notified of offers and services, they have not clarified that this would means that they will stop collecting or sharing the customer's personal information. (IndusInd Privacy Policy, *available at* http://www.indusind.com/indusind/wcms/en/home/footer/privacy-policy/index.html).

[102] RBI, *supra* note 15 (The KYC Norms themselves specify a period of five years, even if the customer terminates his or her account).

[103] Justice AP Shah Committee Report, s*upra* note 75, Ch. 3, Principle 3.

Annexes

Annexure I – Justice AP Shah Committee Report's National Privacy Principles[104]

7.17. The National Privacy Principles should require:

Principle 1: Notice

A data controller shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include:

a) During Collection

- What personal information is being collected;
- Purposes for which personal information is being collected;
- Uses of collected personal information;
- Whether or not personal information may be disclosed to third persons;
- Security safeguards established by the data controller in relation to the personal information;
- Processes available to data subjects to access and correct their own personal information;
- Contact details of the privacy officers and SRO ombudsmen for filing complaints.

b) Other Notices

- Data breaches must be notified to affected individuals and the commissioner when applicable.
- Individuals must be notified of any legal access to their personal information after the purposes of the access have been met.
- Individuals must be notified of changes in the data controller's privacy policy.
- Any other information deemed necessary by the appropriate authority in the interest of the privacy of data subjects.

Principle 2: Choice and Consent

A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. When provision of information is mandated by law, it should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within a reasonable timeframe if published in public databases. As long as the additional transactions are performed within the purpose limitation, fresh consent will not be required.

The data subject shall, at any time while availing the services or otherwise, also have an option to withdraw his/her consent given earlier to the data controller. In such cases the data controller shall have the option not to provide goods or services for which the said information was sought if such information is necessary for providing the goods or services. In exceptional cases, where it is not possible to provide the service with choice and consent, then choice and consent should not be required.

Principle 3: Collection Limitation

A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.

Principle 4: Purpose Limitation

Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.

Principle 5: Access and Correction

[104] Justice AP Shah Committee Report, s*upra* note 75, Ch. 3.

Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data; . Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.

Principle 6: Disclosure of Information

A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.

Principle 7: Security

A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.

Principle 8: Openness

A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

Principle 9: Accountability

The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

Annexure II – Questions Referred to the Bank Officials

Q1. Is the amount and type of information collected directly relevant to the purpose it is collected for?
Q2. Is the collected information mandatorily deleted after the purpose of its collection is satisfied?
Q3. Is an internal audit mechanism in place for checking the efficacy of the privacy measures?
Q4. Is an external audit mechanism in place for checking the efficacy of the privacy measures?
Q5. Is the customer allowed to access the information collected on him or her?
Q6. Are measures to prevent unauthorised access or misuse of information put in place by the bank?

Policy Guide on Privacy in Banking in India

I. Review of Relevant Existing Legislation and Policies

The collection and processing of personal information by Banks in India is regulated by the laws and regulations promulgated by the legislature and the government, and the rules notified by the Reserve Bank of India. Along with these, the Banks are also bound by their own rules and policies, and the standards they choose to subscribe to. The following are the most important rules, regulations, and policies in this regard.

1. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011[1]

Notified by the Central Government under Section 43A of the Information Technology Act, 2000 (hereinafter 'IT Act' or 'Act') read with Section 87 of the Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter 'Rules') are meant to provide basic guidelines that a body corporate or any person who works on their behalf must follow in order to protect the personal and the sensitive personal information of their customers.

These Rules differentiate between Personal Information and Sensitive Personal Information,[2] and only provide protection for the collection, retention, disclosure, and transfer of Sensitive Personal Information. Furthermore, the Rules require body corporate to establish 'reasonable security practices' for the protection of personal information. The Rules refer to ISO 27001 as an example[3] of such standards, which has led to banks relying on ISO 27001. Despite being a recommended standard by the Government, it has been found that the ISO 27001 is practically quite lacking.

2. Master Circular consolidating the Know Your Customer Norms, Anti-Money Laundering Standards, Combating Financial Terrorism and obligations of banks under Prevention of Money Laundering Act, 2002[4]

This Master Circular, notified on the RBI website, consolidates all the obligations of the Indian Banks with regard to their collection and processing of customer information under the Know Your Customer Norms (hereinafter 'KYC Norms'), Anti-Money Laundering Standards (hereinafter 'AML Standards'), Combating Financial Terrorism (hereinafter 'CFT') and obligations of banks under Prevention of Money Laundering Act, 2002 (hereinafter 'PMLA'). These standards require the banks to formulate a KYC Policy that incorporates the following key elements:[5]

1. Customer Acceptance Policy
2. Customer Identification Procedure
3. Monitoring of Transactions
4. Risk Management

Under these norms, banks are required to use strict standards for collecting the identification and address information of their customers, checking customers for possible associations with known offenders or with the "Sanctions Lists" provided to the Bank.[6] Furthermore, banks are required to regularly monitor the transactions of their customers so as to "*[understand] the normal and reasonable activity of the customer*" in order to easily identify unusual behaviour in their account.[7] In this respect, Banks are required to perform ongoing due diligence with respect to their business relationship with every client and examine each client's transactions closely to ensure that they are not outside the expected pattern, which has been developed by what the Bank already knows about the customer.[8] The norms also require banks to group customers according to the risk they present. The extent to which an account is monitored is determined by the category that it falls into.[9] The norms require banks to notify the relevant

---

1 *Available* at http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
2 Personal Information is defined under the Rules, § (1) (i), and Sensitive Personal Information is defined under the Rules, § 3.
3 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011 § 8 (2).
4 *Available at* http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8179.
5 *Id*, § 2.2.
6 *Id*, §§ 2.13 & 2.14 (iv).
7 *Id*, § 2.9.
8 *Id*, § 2.9 (c).
9 *Id.* § 2.3(c).

I. Review of Relevant Existing Legislation and Policies

The collection and processing of personal information by Banks in India is regulated by the laws and regulations promulgated by the legislature and the government, and the rules notified by the Reserve Bank of India. Along with these, the Banks are also bound by their own rules and policies, and the standards they choose to subscribe to. The following are the most important rules, regulations, and policies in this regard.

1. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011[1]

Notified by the Central Government under Section 43A of the Information Technology Act, 2000 (hereinafter 'IT Act' or 'Act') read with Section 87 of the Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter 'Rules') are meant to provide basic guidelines that a body corporate or any person who works on their behalf must follow in order to protect the personal and the sensitive personal information of their customers.

These Rules differentiate between Personal Information and Sensitive Personal Information,[2] and only provide protection for the collection, retention, disclosure, and transfer of Sensitive Personal Information. Furthermore, the Rules require body corporate to establish 'reasonable security practices' for the protection of personal information. The Rules refer to ISO 27001 as an example[3] of such standards, which has led to banks relying on ISO 27001. Despite being a recommended standard by the Government, it has been found that the ISO 27001 is practically quite lacking.

2. Master Circular consolidating the Know Your Customer Norms, Anti-Money Laundering Standards, Combating Financial Terrorism and obligations of banks under Prevention of Money Laundering Act, 2002[4]

This Master Circular, notified on the RBI website, consolidates all the obligations of the Indian Banks with regard to their collection and processing of customer information under the Know Your Customer Norms (hereinafter 'KYC Norms'), Anti-Money Laundering Standards (hereinafter 'AML Standards'), Combating Financial Terrorism (hereinafter 'CFT') and obligations of banks under Prevention of Money Laundering Act, 2002 (hereinafter 'PMLA'). These standards require the banks to formulate a KYC Policy that incorporates the following key elements:[5]

1. Customer Acceptance Policy
2. Customer Identification Procedure
3. Monitoring of Transactions
4. Risk Management

Under these norms, banks are required to use strict standards for collecting the identification and address information of their customers, checking customers for possible associations with known offenders or with the "Sanctions Lists" provided to the Bank.[6] Furthermore, banks are required to regularly monitor the transactions of their customers so as to "*[understand] the normal and reasonable activity of the customer*" in order to easily identify unusual behaviour in their account.[7] In this respect, Banks are required to perform ongoing due diligence with respect to their business relationship with every client and examine each client's transactions closely to ensure that they are not outside the expected pattern, which has been developed by what the Bank already knows about the customer.[8] The norms also require banks to group customers according to the risk they present. The extent to which an account is monitored is determined by the category that it falls into.[9] The norms require banks to notify the relevant

1 *Available* at http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
2 Personal Information is defined under the Rules, § (1) (i), and Sensitive Personal Information is defined under the Rules, § 3.
3 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011 § 8 (2).
4 *Available at* http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8179.
5 *Id*, § 2.2.
6 *Id*, §§ 2.13 & 2.14 (iv).
7 *Id*, § 2.9.
8 *Id*, § 2.9 (c).
9 *Id.* § 2.3(c).

Policy Guide on Privacy in Banking in India

I. Review of Relevant Existing Legislation and Policies

The collection and processing of personal information by Banks in India is regulated by the laws and regulations promulgated by the legislature and the government, and the rules notified by the Reserve Bank of India. Along with these, the Banks are also bound by their own rules and policies, and the standards they choose to subscribe to. The following are the most important rules, regulations, and policies in this regard.

1. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011[1]

Notified by the Central Government under Section 43A of the Information Technology Act, 2000 (hereinafter 'IT Act' or 'Act') read with Section 87 of the Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter 'Rules') are meant to provide basic guidelines that a body corporate or any person who works on their behalf must follow in order to protect the personal and the sensitive personal information of their customers.

These Rules differentiate between Personal Information and Sensitive Personal Information,[2] and only provide protection for the collection, retention, disclosure, and transfer of Sensitive Personal Information. Furthermore, the Rules require body corporate to establish 'reasonable security practices' for the protection of personal information. The Rules refer to ISO 27001 as an example[3] of such standards, which has led to banks relying on ISO 27001. Despite being a recommended standard by the Government, it has been found that the ISO 27001 is practically quite lacking.

2. Master Circular consolidating the Know Your Customer Norms, Anti-Money Laundering Standards, Combating Financial Terrorism and obligations of banks under Prevention of Money Laundering Act, 2002[4]

This Master Circular, notified on the RBI website, consolidates all the obligations of the Indian Banks with regard to their collection and processing of customer information under the Know Your Customer Norms (hereinafter 'KYC Norms'), Anti-Money Laundering Standards (hereinafter 'AML Standards'), Combating Financial Terrorism (hereinafter 'CFT') and obligations of banks under Prevention of Money Laundering Act, 2002 (hereinafter 'PMLA'). These standards require the banks to formulate a KYC Policy that incorporates the following key elements:[5]

1. Customer Acceptance Policy
2. Customer Identification Procedure
3. Monitoring of Transactions
4. Risk Management

Under these norms, banks are required to use strict standards for collecting the identification and address information of their customers, checking customers for possible associations with known offenders or with the "Sanctions Lists" provided to the Bank.[6] Furthermore, banks are required to regularly monitor the transactions of their customers so as to "*[understand] the normal and reasonable activity of the customer*" in order to easily identify unusual behaviour in their account.[7] In this respect, Banks are required to perform ongoing due diligence with respect to their business relationship with every client and examine each client's transactions closely to ensure that they are not outside the expected pattern, which has been developed by what the Bank already knows about the customer.[8] The norms also require banks to group customers according to the risk they present. The extent to which an account is monitored is determined by the category that it falls into.[9] The norms require banks to notify the relevant

1 *Available* at http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
2 Personal Information is defined under the Rules, § (1) (i), and Sensitive Personal Information is defined under the Rules, § 3.
3 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules), 2011 § 8 (2).
4 *Available at* http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8179.
5 *Id*, § 2.2.
6 *Id*, §§ 2.13 & 2.14 (iv).
7 *Id*, § 2.9.
8 *Id*, § 2.9 (c).
9 *Id.* § 2.3(c).

		SBI		CBI		IndusInd		ICICI		SCB		Comments
Notice		Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Abbreviations used: Account Opening Forms - AOF
Is the customer notified of all types of information that are collected?		No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Link to BCSBI's Code of Banks' Commitment to Customers: http://www.bcsbi.org.in/Codes_CommitmentCustomers.html
Is the customer notified of the purposes for which the information is collected?		No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Is the customer notified through the forms or any other documents of the method in which he may access the collected information?		No	No	No	No	No	No	No	No	-	No	
Is the customer notified of the methods in which he may correct or withdraw collected information?		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	-	No	
Is the customer notified of the security regulations put in place by the bank for the protection of the collected information?		No	No	No	No	No	No	No	No	-	No	
Choice and Consent												
Is the customer allowed to opt out of collection of non-mandatory information?		No	No	No	No	No	No	Yes	No	-	No	
Is the customer allowed to withdraw consent once it is given?		No	No	No	No	No	No	No	No	-	No	
Collection Limitation												
Is the information collected limited to that which the customer is informed of?		No	Yes	No	Yes	Yes	Yes	Yes	Yes	-	Yes	
Purpose Limitation												
Is the amount and type of information collected directly relevant to the purpose it is collected for?		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	Yes	
Is the collected information mandatorily deleted after a the purpose of its collection is satisfied?		No	No	No	No	No	No	No	No	-	No	
Is there a provison for informing the customer in case there is a change in the purpose for which the information is collected?		Yes	No	Yes	No	No	No	Yes	No	-	No	
Access and Correction												
Is the customer allowed to access the information collected on him or her?		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	Yes	

		SBI		CBI		IndusInd		ICICI		SCB		Comments
Notice		Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Abbreviations used: Account Opening Forms - AOF
Is the customer allowed to amend or correct any errors in the information collected on him or her, or delete any incorrect information?		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	-	Yes	
Is the customer able to confirm if the bank is holding or processing any personal information about him or her with exception to the above?		No	No	No	No	No	No	No	No	-	No	
In case the above is yes, can a copy be obtained?		No	No	No	No	No	No	No	No	-	No	
Disclosure of Information												
Is the customer notified of all the circumstances in which the information may be disclosed and to whom?		Yes	Yes	No	Yes	Yes	Yes	No	Yes	-	Yes	
Is the customer informed of the type and extent of the information that is mandatorily shared with authorised bodies?		No	No	No	No	Yes	No	No	No	-	No	
Is the customer informed of the type and extent of from the collected information that will be available publically?		No	No	No	No	No	No	No	No	-	No	
Is the customer allowed to not consent to sharing information with non-authorised agencies?		No	No	No	No	No	No	Yes	No	-	No	
Does the bank inform the customer of the laws which govern the disclosure of information?		No	Yes	No	No	Yes	No	No	No	-	No	
Security												
Are the security measures put in place to ensure the safety of the collected information adequately specified in the forms?		No	No	No	No	No	No	No	No	-	No	
Are measures to prevent unauthorised access or misuse of information put in place by the bank?		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	Yes	
Openness												
Is the information made available to the customer easily intelligible?		Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	-	Yes	
Is the given information reasonably detailed?		No	No	No	No	Yes	No	No	No		No	
Accountability												
Is an internal audit mechanism in place for checking the efficacy of the privacy measures?		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	(Refused to answer the question)	

		SBI		CBI		IndusInd		ICICI		SCB		Comments
Notice		Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Abbreviations used: Account Opening Forms - AOF
Is an external audit mechanism in place for checking the efficacy of the privacy measures?		-	-	-	-	-	-	-	-	-	-	
Is there a grievance redressal mechanism in place?		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Is there an assigned officer in charge of addressing and managing privacy concerns?		No	No	No	No	No	No	No	No	No	No	
Total Positives (of 26)		10	13	11	11	15	12	14	10	-	10	
Relevant Links:	AOF/Loan Application Form:	http://www.sbi.co.in/webfiles/uploads/files/1295443117344-AccountOpeningForm-EN.pdf	Hard copy obtained from bank	https://www.central-bankofindia.co.in/upload/AOF%20-Personal%20AC%20Form-c2c.pdf	https://www.centralbanko-findia.co.in/upload/Com-mon_Application.pdf	http://www.indusind.com/indusind/wcms/en/home/top-links/forms-center/accountopeningforms/index.avsFiles/PDF/SA%20(AOF)%20_%20SB%20form%20Ver-sion%202%20_%2016-12-2013%20_%20Final.pdf	Hard copy obtained from bank	Hard copy obtained from bank	Hard copy obtained from bank	The AOF could not be obtained for this bank. The respones are based on whatever documents could be obtained.	https://www.sc.com/in/_documents/tools-utilities/form-centre/Personal%20Loan%20Application%20Form.pdf	
	Most Important Terms and Conditions		https://www.sbi.co.in/webfiles/uploads/files/1377606055343_HOME_LOAN_MITC.pdf									
	KYC Documentation			(KYC Documentation) https://www.central-bankofindia.co.in/upload/Copy%20of%20kyc%20english.pdf		http://www.indusind.com/indusind/wcms/en/home/top-links/forms-center/accountopeningforms/cd-checklist.avsFiles/PDF/Instructions%20and%20Checklist%20CDS%20AOF.pdf		http://www.icicibank.com/notice-board/Know_Your_Customer.pdf	http://www.icicibank.com/notice-board/Know_Your_Customer.pdf			
	KYC Documentation			(KYC requirements for an SB Account) www.centralbankofindia.co.in/upload/KYC.pdf'		(KYC Policy)http://www.indusind.com/indusind/wcms/en/home/important-links/kyc/index.html						
	KYC Documentation					(KYC FAQ) http://www.indusind.com/indusind/wcms/en/home/customer-care/faq/index.html?bankingType=KYC%20&%20AML						
	KYC Documentation					(KYC Declaration Form) http://www.indusind.com/indusind/wcms/en/home/important-links/kyc/kyc_declaration_form.pdf						
	Other Documentation			(Customer Information Form) https://www.cen-tralbankofindia.co.in/up-load/CIF%20Personal%20AC%20Form-c2c.pdf		http://www.indusind.com/indusind/wcms/en/home/personal-banking/ac-counts/Savings-Accounts-TnC-V31.pdf						

		SBI		CBI		IndusInd		ICICI		SCB		Comments
Notice		Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Opening an Account	Taking a Personal Loan	Abbreviations used: Account Opening Forms - AOF
	Grievances and Complaints	https://www.sbi.co.in/user.htm?action=viewsection&lang=0&id=0,453,14	(Grievance Redressal Policy) https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDQQFjAB&url=https%3A%2F%2Fwww.sbi.co.in%2Fwebfiles%2Fuploads%2Ffiles%2F1339585079004_GRIEVANCE_REDRESSAL_POLICY_JAN_2012.pdf&ei=3US9UpSUB46qrAeatIHQBA&usg=AFQjCNGSxdq53RiAgdzf7c97EtQKXmEoOg&sig2=pT4b9tLCAgZNlwXWU7RppQ&bvm=bv.58187178,d.bmk	(Online Complaint form) https://www.centralbankofindia.co.in/Site/mainsite.aspx?status=l1&menu_id=90	(List of Nodal Officers for Complaints) https://www.centralbankofindia.co.in/upload/Copy%20of%20Copy%20of%20NODAL%20OFFICERS.xls	http://www.indusind.com/indusind/wcms/en/home/important-links/corporate-governance/grievance-redressaland-complaintform/index.html	http://www.indusind.com/indusind/wcms/en/home/important-links/corporate-governance/grievance-redressaland-complaintform/index.html	(Grievance Redressal Policy) http://www.icicibank.com/notice-board/customergrievance-redressal-policy.pdf	(Grievance Redressal Policy) http://www.icicibank.com/notice-board/customergrievance-redressal-policy.pdf	https://www.sc.com/in/help-centre/complaints.html	https://www.sc.com/in/help-centre/complaints.html	
			http://www.sbi.co.in/webfiles/uploads/files/1348749777896_GRIEVANCE_REDRESSAL_STEP_BY_STEP_NEW.pdf									
	Privacy Policy					http://www.indusind.com/indusind/wcms/en/home/footer/privacy-policy/index.html		http://www.icicibank.com/privacy.html				