Privacy Policy

Union Bank of India

Data Protection Office

1. Introduction

We, **Union Bank of India (hereinafter referred to as “the Bank” or “UBI”)**, are committed to protecting the privacy of the Bank’s customers’ data including Personal Data and have taken all necessary measures to safeguard it. Keeping information secure is one of the banks most important responsibilities.

The Bank maintains **physical, electronic, and procedural safeguards** to protect customers’ data including Personal Data. Access to such information is strictly limited to employees, **authorized service providers**, and other vendors for lawful purposes only. All employees and authorized service providers are bound by a **code of ethics** that mandates the confidential treatment of customer information, and any violation of this code is subject to disciplinary action.

The Bank shall not be held liable for disclosure of confidential information when such disclosure is:

- In accordance with this Privacy Policy (or Policy),
- As per agreements with customers, or
- In compliance with applicable laws or directives from competent authorities.

The Bank recognizes and upholds the responsibility to maintain the confidentiality of all information entrusted to us by our customers.

Scope of this Privacy Policy

- This Privacy Policy (“document”) applies when the services of the Bank are availed either directly or through merchant partners for any financial or non-financial transaction with the Bank.
- This Notice is framed to outline the Bank’s broader commitment to maintaining high standards of privacy and responsible data handling. It sets forth the privacy practices followed by the Bank and the manner in which the Bank collects, uses, discloses, stores, secures, and disposes of Information/Data including your Personal Data and Sensitive Personal Data, whether processed in physical or electronic form. Further, this Notice also reflects the Bank’s approach to meeting its obligations under applicable laws, including the Digital Personal Data Protection Act, 2023.Throughout this document, the terms **“we”, “us”, “our” & “ours”** refer to UBI, and the terms **“you”, “your” & “yours”** refer to the individual whose data including Personal Data is being processed.

Definitions

Application: The Bank’s mobile application or any other application through which the Bank’s services can be availed electronically.

Personal Data: Any information relating to an individual that can identify such person directly or indirectly, in combination with other information available or likely to be available with the Bank.

Sensitive Personal Data: It is a subset of Personal Data. Wherever Sensitive Personal Data is not mentioned separately, it is deemed included under Personal Data.

Sensitive Personal Data or Information includes:

1. Financial information such as bank account, credit/debit card details, or other payment instrument details
2. Physical, physiological, and mental health condition
3. Medical records and history
4. Biometric information
5. Password
6. Any information received under the above clauses for processing, stored or processed under lawful contract or otherwise
7. Any other information which may fall under the ambit of Sensitive Personal Data (as defined by the Bank from time to time).

Website: A collection of publicly accessible, interlinked web pages of the Bank under a single domain name, created and maintained for various purposes.

2. Applicability

This is applicable Data and/or Information including Personal Data and Sensitive Personal Data collected and processed by us or is received directly from you at our offices/branches or through the Bank's website, applications and electronic communications and any information collected by the Bank's server from the browser, or the physical forms that are later digitized.

Exceptions of Personal Data/Sensitive Personal Data-

- Any information freely available in the public domain
- Any reviews, comments, messages, or blogs posted by customers on public sections of the Bank's website or application become published content and are not considered personal or sensitive data subject to this document.

3. What Data including Personal Data does the Bank Collect & Process?

The Bank collects the following categories of Data including Personal Data for providing services to you. Please note below is not an exhaustive list and may change as per the products and services offered to fulfil regulatory and legal requirements:

a) Demographic & Identification Data

i. Name, first name, middle name, last name
ii. Date of birth, age, gender, marital status, nationality, religion, caste
iii. Contact details: address (home, permanent, residential), phone numbers, email IDs
iv. Depositor name, director name, director address, guarantor name, spouse's name, father's name, mother's maiden name

v. Nominee and beneficiary details (name, relationship, date of birth, address)
vi. Photograph, signature, CCTV footage, location data
vii. Identity and address proof: Aadhaar, PAN, passport, voter ID, driving license, KYC documents, CIF ID
viii. Employment details, education qualifications

b) ***Financial Information***

i. Bank account details, account number, IFSC code
ii. Account statements, transaction history
iii. Annual income, salary slips, income tax returns (Form 16)
iv. Loan details: amount, sanction date
v. Credit score (e.g., CIBIL), net worth statements, PF number
vi. Card details (credit/debit), payment instrument information

4. Where does the bank obtain Data from?

Most of the Data including Personal Data processed by the Bank is provided directly by you through our website, mobile banking application, by visiting our branches, through our authorised third parties (such as DSAs and CSAs), or through Relationship Managers, and while using our products and services. We may also collect certain information through cookies when you visit our website. In addition, we may collect information about you from other sources as described below, and after verifying its authenticity, may add it to the data we already hold and process it in accordance with this Privacy Policy.

If Personal Data is collected from third-party service providers for the purpose of offering relevant marketing content, offers, or services, such data will be used and processed only with your consent. These third-party service providers may include email service providers, and public data bases, social media sites as well as other third parties as deemed appropriate. We, including our service providers, may monitor, record & retain your image, conversations and/ or electronic communication between you & us electronically or otherwise as deemed appropriate.

5. Purpose for collecting and processing Data including Personal Data

The Bank processes your Data including Personal Data for the following purposes:

- Provide products and assist in and administer the provision of services to you, which includes activities like account opening, product delivery, onboarding, and service facilitation:

- To process account opening (in person, branch assisted, VKYC)
- To issue and deliver credit cards/debit cards
- UIDAI Aadhaar Verification
- To onboard clients and partners for banking and financial services
- To facilitate NEFT transactions, NACH mandates, and digital/physical payments

- To manage locker facilities and cheque books
- To deliver services via call centre and doorstep banking
- To maintain records and reconcile accounts
- To provide financial literacy training and general services
- To onboard buyers for TReDS and clients for channel finance
- To evaluate and onboard loan accounts from NBFCs
- To facilitate joint loan disbursement
- To generate financial statements and maintain borrower accounts
- To provide general banking services

➢ Prevent, detect, investigate and prosecute fraud and alleged fraud, money laundering and other crimes and to verify your identity which includes KYC, compliance, and fraud related activities:

- Includes KYC, compliance, and fraud-related activities:
- To verify and update customer contact details
- To conduct due diligence and investigations
- To fulfil legal obligations and provide data to auditors
- To facilitate Re-KYC and investigate staff accountability
- To monitor and manage stressed loan accounts
- To identify early signs of financial distress

➢ Providing information about products, offers, promotions, and services, which includes marketing and outreach activities in accordance with the consent provided by you.

➢ Process and deal with any complaints or enquiries made by or about you which includes grievance redressal and customer support:

- To handle customer complaints and RCA
- To recover the dues
- To resolve GST-related complaints
- To investigate and redress grievances
- To reach out to customers to recover the loans
- To ensure secure and efficient recovery of dues

➢ To analyse your Personal Data for Anti-Money Laundering (AML) and other regulatory compliance requirements, provisioning of services, assessing loan and credit eligibility, and for other legitimate purposes necessary to support the Bank’s operations.

➢ For reporting to regulatory authorities and internal audits

6. Sharing of Personal Data

The Bank may disclose your Personal Data to various categories of third parties after obtaining your consent for the same or as part of legitimate use as per DPDPA. However, the Bank may also disclose your Personal Data without your consent where such disclosure is required under applicable laws, where the Bank is mandated to cooperate with statutory, regulatory, or governmental authorities, or where such disclosure is necessary for the legitimate use under the DPDP Act. The third parties include:

- **Other Group Companies, Partners, and Subsidiaries** for providing or enhancing products, services, and customer experience.
- **Sub-contractors, agents, or service providers** who work for the Bank or provide services/products on behalf of the Bank.
- **Partners offering co-branded services, products, or programs**, where such sharing is necessary to deliver the offering.
- **Agents or service providers** engaged for activities connected to customer servicing, operational support, marketing (where permissible), or other contractual obligations.
- **Law enforcement agencies**, **government authorities**, **investigating agencies**, and any authority empowered under law.
- **Regulators**, including the **Reserve Bank of India**, Indian or overseas regulatory bodies, auditors, and entities appointed by regulators to conduct inspections, audits, or investigations.
- **Courts, tribunals, judicial or quasi-judicial bodies**, arbitrators, and arbitration tribunals.
- **Credit information companies / credit bureaus**, statutory bodies, and any persons or entities to whom disclosure is mandatory under applicable laws.
- Situations involving **regulatory reporting**, compliance with legal processes, or to **assert or defend the Bank's legal rights and interests**.

7. Withdrawal of Consent

Any individual has the right to withdraw their consent for the processing of their Personal Data at any time. Such withdrawal applies specifically to processing carried out for purposes, such as marketing or promotional communications, and will take effect only for future processing activities. It will not affect the lawfulness of any processing that was carried out prior to the withdrawal of consent. Even after consent is withdrawn, the Bank may continue to process Personal Data where required to comply with legal or regulatory obligations, to protect the Bank's lawful interests, to pursue available remedies, or to defend against existing or potential claims.

In accordance with the requirements of the Digital Personal Data Protection Act, 2023, a clear and accessible mechanism for withdrawal of consent is required. Data Principals may withdraw or modify their consent at any time by using the consent management option available on the corporate website, internet banking portal, mobile banking application, among others.

8. Processing of Personal Data of Children and Persons with Disability

We obtain verifiable consent from a parent or lawful guardian before processing the Personal Data of minors. We ensure that such processing does not have any detrimental effect on the child's well-being. The Bank does not engage in profiling, behavioural monitoring, or targeted advertising directed at children, and their data is not used for marketing or promotional activities. In line with the principle of data minimisation, only essential information required for providing the requested services is collected.

Where the individual is a Person with Disability who is unable to provide legally valid consent, we obtain verifiable consent from the lawful guardian before processing their Personal Data. Such processing is carried out with due care to ensure that it does not adversely impact the individual's well-being.

9. Use of Cookies

- We use cookies and similar technologies to enhance your browsing experience, analyse site traffic, and personalised content. Some cookies are essential for this site to function, while others help us understand your use and preferences enabling us to improve our services. These are stored locally on your computer or mobile devices. By clicking "Accept All", you consent to the storage of cookies on your device & its functionality in accordance with our Cookie Policy. To customize your cookie preference, click "Customize" and select the categories you want to accept. You may choose to manage your preferences or modify/ withdraw your consent at any time by accessing cookie settings in your device.
- The Bank is not responsible for cookies placed in the device of user/s by any other website and data including Personal Data collected thereto. We do not control these cookies and once you have clicked on the advertisement and left the site, our Privacy Policy no longer applies.

10. Data Security

- The Bank is committed to protecting your Information/Data including your Personal Data and Sensitive Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your data including Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your data including Personal Data is executed with the third parties/ vendors/ service providers involved in providing services to us.
- The Bank has adopted ISO/IEC 27001 standard, which is a globally accepted standard. The Bank's Data centres, IT and Support functions are ISO 27001:2013 certified.

11. Data Principal Rights

We are committed to ensuring that you are aware of and can exercise your rights regarding your personal Data

Data principals have the following rights about their personal Data:

- **Right of Access**: Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification**: Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure**: Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate**: Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights. When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights, customer can visit corporate website, internet banking portal, mobile banking application, among others and can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations.

12. Retention of Personal Data

The Bank may retain your Personal Data for as long as required for legitimate purposes that may include such as managing your account and dealing with any concerns that may arise or otherwise if as may be required for any for legal, regulatory and/or statutory reasons.

If the Bank no longer requires the retention of the information provided by the Customer, it will use best efforts to destroy or delete such Customer Information as per our Bank's internal policies.

13. Links to other Websites and Social Media

The Bank website may contain links to websites of other organizations that are not owned by Bank. This document does not cover how those organizations process your data including

Personal Data. We encourage you to read the relevant privacy notice/policy on the other websites that you may visit.

Please note that when visiting Bank's official social media site/ page, you are subject to this document well as the social media platform's own terms and conditions.

14. Conflict of Laws & Disputes

You agree that, irrespective of your location or country of jurisdiction, this document and its contents shall be subject to and governed by Indian laws (as amended from time to time) as may be applicable and that you waive all your rights which you may have in relation to this document under any contract or relevant laws applicable to the jurisdiction where you are situated and/or by which you are governed.

Any disputes over inter alia collection, storage and handling of data including Personal Data will be governed by this document, Terms and Conditions and by the laws of India and courts of India shall have exclusive jurisdiction.

15. Grievance Redressal

In case of any discrepancies or grievances, you may contact us at

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

16. Notification of Changes

We may update this Privacy Policy from time to time to reflect changes in our business, technology, or legal requirements. We encourage you to review this Privacy Policy regularly to stay informed about our privacy practices and any changes we may make.

This Privacy Policy was last updated on July 31, 2026.

Privacy Notice

Union Bank of India

Data Protection Office

1. Introduction

We, **Union Bank of India (hereinafter referred to as "the Bank" or "UBI")**, are committed to protecting the privacy of the Bank's customers' data including Personal Data and have taken all necessary measures to safeguard it. Keeping information secure is one of the banks most important responsibilities.

The Bank maintains **physical, electronic, and procedural safeguards** to protect customers' data including Personal Data. Access to such information is strictly limited to employees, **authorized service providers**, and other vendors for lawful purposes only. All employees and authorized service providers are bound by a **code of ethics** that mandates the confidential treatment of customer information, and any violation of this code is subject to disciplinary action.

The Bank shall not be held liable for disclosure of confidential information when such disclosure is:

- In accordance with this Privacy Notice (or Notice),
- As per agreements with customers, or
- In compliance with applicable laws or directives from competent authorities.

The Bank recognizes and upholds the responsibility to maintain the confidentiality of all information entrusted to us by our customers.

Scope of this Privacy Notice

- This Privacy Notice ("document") applies when the services of the Bank are availed either directly or through merchant partners for any financial or non-financial transaction with the Bank.
- This Notice is framed to outline the Bank's broader commitment to maintaining high standards of privacy and responsible data handling. It sets forth the privacy practices followed by the Bank and the manner in which the Bank collects, uses, discloses, stores, secures, and disposes of Information/Data including your Personal Data and Sensitive Personal Data, whether processed in physical or electronic form. Further, this Notice also reflects the Bank's approach to meeting its obligations under applicable laws, including the Digital Personal Data Protection Act, 2023.Throughout this document, the terms **"we", "us", "our" & "ours"** refer to UBI, and the terms **"you", "your" & "yours"** refer to the individual whose data including Personal Data is being processed.

Definitions

Application: The Bank's mobile application or any other application through which the Bank's services can be availed electronically.

Personal Data: Any information relating to an individual that can identify such person directly or indirectly, in combination with other information available or likely to be available with the Bank.

Sensitive Personal Data: It is a subset of Personal Data. Wherever Sensitive Personal Data is not mentioned separately, it is deemed included under Personal Data.
Sensitive Personal Data or Information includes:

a. Financial information such as bank account, credit/debit card details, or other payment instrument details
b. Physical, physiological, and mental health condition
c. Medical records and history
d. Biometric information
e. Password
f. Any information received under the above clauses for processing, stored or processed under lawful contract or otherwise
g. Any other information which may fall under the ambit of Sensitive Personal Data (as defined by the Bank from time to time).

Website: A collection of publicly accessible, interlinked web pages of the Bank under a single domain name, created and maintained for various purposes.

2. Applicability

This is applicable Data and/or Information including Personal Data and Sensitive Personal Data collected and processed by us or is received directly from you at our offices/branches or through the Bank's website, applications and electronic communications and any information collected by the Bank's server from the browser, or the physical forms that are later digitized.

Exceptions of Personal Data/Sensitive Personal Data-

i. Any information freely available in the public domain
ii. Any reviews, comments, messages, or blogs posted by customers on public sections of the Bank's website or application become published content and are not considered personal or sensitive data subject to this document.

3. What Data including Personal Data does the Bank Collect & Process?

The Bank collects the following categories of Data including Personal Data for providing services to you. Please note below is not an exhaustive list and may change as per the products and services offered to fulfil regulatory and legal requirements:

Demographic & Identification Data

i. Name, first name, middle name, last name
ii. Date of birth, age, gender, marital status, nationality, religion, caste
iii. Contact details: address (home, permanent, residential), phone numbers, email IDs

iv. Depositor name, director name, director address, guarantor name, spouse's name, father's name, mother's maiden name
v. Nominee and beneficiary details (name, relationship, date of birth, address)
vi. Photograph, signature, CCTV footage, location data
vii. Identity and address proof: Aadhaar, PAN, passport, voter ID, driving license, KYC documents, CIF ID
viii. Employment details, education qualifications

Financial Information

a. Bank account details, account number, IFSC code
b. Account statements, transaction history
c. Annual income, salary slips, income tax returns (Form 16)
d. Loan details: amount, sanction date
e. Credit score (e.g., CIBIL), net worth statements, PF number
f. Card details (credit/debit), payment instrument information

4. Where does the bank obtain Data from?

Most of the Data including Personal Data processed by the Bank is provided directly by you through our website, mobile banking application, by visiting our branches, through our authorised third parties (such as DSAs and CSAs), or through Relationship Managers, and while using our products and services. We may also collect certain information through cookies when you visit our website. In addition, we may collect information about you from other sources as described below, and after verifying its authenticity, may add it to the data we already hold and process it in accordance with this Privacy Notice.

If Personal Data is collected from third-party service providers for the purpose of offering relevant marketing content, offers, or services, such data will be used and processed only with your consent. These third-party service providers may include email service providers, and public data bases, social media sites as well as other third parties as deemed appropriate. We, including our service providers, may monitor, record & retain your image, conversations and/ or electronic communication between you & us electronically or otherwise as deemed appropriate.

5. Purpose for collecting and processing Data including Personal Data

The Bank processes your Data including Personal Data for the following purposes:

- ➢ Provide products and assist in and administer the provision of services to you, which includes activities like account opening, product delivery, onboarding, and service facilitation:
- To process account opening (in person, branch assisted, VKYC)
- To issue and deliver credit cards/debit cards

- UIDAI Aadhaar Verification
- To onboard clients and partners for banking and financial services
- To facilitate NEFT transactions, NACH mandates, and digital/physical payments
- To manage locker facilities and cheque books
- To deliver services via call centre and doorstep banking
- To maintain records and reconcile accounts
- To provide financial literacy training and general services
- To onboard buyers for TReDS and clients for channel finance
- To evaluate and onboard loan accounts from NBFCs
- To facilitate joint loan disbursement
- To generate financial statements and maintain borrower accounts
- To provide general banking services

➢ Prevent, detect, investigate and prosecute fraud and alleged fraud, money laundering and other crimes and to verify your identity which includes KYC, compliance, and fraud related activities:

- Includes KYC, compliance, and fraud-related activities:
- To verify and update customer contact details
- To conduct due diligence and investigations
- To fulfil legal obligations and provide data to auditors
- To facilitate Re-KYC and investigate staff accountability
- To monitor and manage stressed loan accounts
- To identify early signs of financial distress

➢ Providing information about products, offers, promotions, and services, which includes marketing and outreach activities in accordance with the consent provided by you.

➢ Process and deal with any complaints or enquiries made by or about you which includes grievance redressal and customer support:

- To handle customer complaints and RCA
- To recover the dues
- To resolve GST-related complaints
- To investigate and redress grievances
- To reach out to customers to recover the loans
- To ensure secure and efficient recovery of dues

➢ To analyse your Personal Data for Anti-Money Laundering (AML) and other regulatory compliance requirements, provisioning of services, assessing loan and credit eligibility, and for other legitimate purposes necessary to support the Bank's operations.

➢ For reporting to regulatory authorities and internal audits

6. Sharing of Personal Data

The Bank may disclose your Personal Data to various categories of third parties after obtaining your consent for the same or as part of legitimate use as per DPDPA. However, the Bank may also disclose your Personal Data without your consent where such disclosure is required under applicable laws, where the Bank is mandated to cooperate with statutory, regulatory, or governmental authorities, or where such disclosure is necessary for the legitimate use under the DPDP Act. The third parties include:

- **Other Group Companies, Partners, and Subsidiaries** for providing or enhancing products, services, and customer experience.
- **Sub-contractors, agents, or service providers** who work for the Bank or provide services/products on behalf of the Bank.
- **Partners offering co-branded services, products, or programs**, where such sharing is necessary to deliver the offering.
- **Agents or service providers** engaged for activities connected to customer servicing, operational support, marketing (where permissible), or other contractual obligations.
- **Law enforcement agencies**, **government authorities**, **investigating agencies**, and any authority empowered under law.
- **Regulators**, including the **Reserve Bank of India**, Indian or overseas regulatory bodies, auditors, and entities appointed by regulators to conduct inspections, audits, or investigations.
- **Courts, tribunals, judicial or quasi-judicial bodies**, arbitrators, and arbitration tribunals.
- **Credit information companies / credit bureaus**, statutory bodies, and any persons or entities to whom disclosure is mandatory under applicable laws.
- Situations involving **regulatory reporting**, compliance with legal processes, or to **assert or defend the Bank's legal rights and interests**.

7. Withdrawal of Consent

Any individual has the right to withdraw their consent for the processing of their Personal Data at any time. Such withdrawal applies specifically to processing carried out for purposes, such as marketing or promotional communications, and will take effect only for future processing activities. It will not affect the lawfulness of any processing that was carried out prior to the withdrawal of consent. Even after consent is withdrawn, the Bank may continue to process Personal Data where required to comply with legal or regulatory obligations, to protect the Bank's lawful interests, to pursue available remedies, or to defend against existing or potential claims.

In accordance with the requirements of the Digital Personal Data Protection Act, 2023, a clear and accessible mechanism for withdrawal of consent is required. Data Principals may withdraw or modify their consent at any time by using the consent management option available on the corporate website, internet banking portal, mobile banking application, among others.

8. Processing of Personal Data of Children and Persons with Disability

We obtain verifiable consent from a parent or lawful guardian before processing the Personal Data of minors. We ensure that such processing does not have any detrimental effect on the child's well-being. The Bank does not engage in profiling, behavioural monitoring, or targeted advertising directed at children, and their data is not used for marketing or promotional activities. In line with the principle of data minimisation, only essential information required for providing the requested services is collected.

Where the individual is a Person with Disability who is unable to provide legally valid consent, we obtain verifiable consent from the lawful guardian before processing their Personal Data. Such processing is carried out with due care to ensure that it does not adversely impact the individual's well-being.

9. Use of Cookies

- We use cookies and similar technologies to enhance your browsing experience, analyse site traffic, and personalised content. Some cookies are essential for this site to function, while others help us understand your use and preferences enabling us to improve our services. These are stored locally on your computer or mobile devices. By clicking "Accept All", you consent to the storage of cookies on your device & its functionality in accordance with our Cookie Policy. To customize your cookie preference, click "Customize" and select the categories you want to accept. You may choose to manage your preferences or modify/ withdraw your consent at any time by accessing cookie settings in your device.
- The Bank is not responsible for cookies placed in the device of user/s by any other website and data including Personal Data collected thereto. We do not control these cookies and once you have clicked on the advertisement and left the site, our Privacy Notice no longer applies.

10. Data Security

- The Bank is committed to protecting your Information/Data including your Personal Data and Sensitive Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your data including Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your data including Personal Data is executed with the third parties/ vendors/ service providers involved in providing services to us.
- The Bank has adopted ISO/IEC 27001 standard, which is a globally accepted standard. The Bank's Data centres, IT and Support functions are ISO 27001:2013 certified.

11. Data Principal Rights

We are committed to ensuring that you are aware of and can exercise your rights regarding your personal Data

Data principals have the following rights about their personal Data:

- **Right of Access**: Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification**: Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure**: Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate**: Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights. When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights, customer can visit corporate website, internet banking portal, mobile banking application, among others and can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations.

12. Retention of Personal Data

The Bank may retain your Personal Data for as long as required for legitimate purposes that may include such as managing your account and dealing with any concerns that may arise or otherwise if as may be required for any for legal, regulatory and/or statutory reasons.

If the Bank no longer requires the retention of the information provided by the Customer, it will use best efforts to destroy or delete such Customer Information as per our Bank's internal policies.

13. Links to other Websites and Social Media

The Bank website may contain links to websites of other organizations that are not owned by Bank. This document does not cover how those organizations process your data including Personal Data. We encourage you to read the relevant privacy notice on the other websites that you may visit.

Please note that when visiting Bank's official social media site/ page, you are subject to this document well as the social media platform's own terms and conditions.

14. Conflict of Laws & Disputes

You agree that, irrespective of your location or country of jurisdiction, this document and its contents shall be subject to and governed by Indian laws (as amended from time to time) as may be applicable and that you waive all your rights which you may have in relation to this document under any contract or relevant laws applicable to the jurisdiction where you are situated and/or by which you are governed.

Any disputes over inter alia collection, storage and handling of data including Personal Data will be governed by this document, Terms and Conditions and by the laws of India and courts of India shall have exclusive jurisdiction.

15. Grievance Redressal

In case of any discrepancies or grievances, you may contact us at

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

16. Notification of Changes

We may update this Privacy Notice from time to time to reflect changes in our business, technology, or legal requirements. We encourage you to review this Privacy Notice regularly to stay informed about our privacy practices and any changes we may make.

This Privacy Notice was last updated on July 31, 2026

Visitor Privacy Notice

Introduction

Welcome to Union Bank of India (hereafter known as 'Bank' or 'UBI'), we are committed to protecting and respecting your privacy. This visitor privacy notice describes your privacy rights in relation to the information/data about you that we process as well as the steps we take to protect your privacy.

If you have questions or comments about our administration of your personal data, please contact us at dpoffice@unionbankofindia.bank.in You may also use this address to communicate any concerns you may have regarding compliance with our Privacy Statement.

Visitor means any individual who is not a permanent employee of Union Bank of India and who enters, seeks to enter, or is present within the Bank's premises (including offices, branches, data centres, or other controlled facilities), whether temporarily or for a specific purpose.

This includes, but is not limited to:

- Vendors, contractors, consultants, auditors, and service providers
- Government or regulatory officials
- Business associates, partners, and guests
- Any other persons granted physical or electronic access to the Bank's premises, systems, or facilities

A Visitor may be required to provide personal data, including identification and electronic identification information, for purposes such as security, access control, verification, compliance, and record-keeping, as described in this Visitor Privacy Notice.

Collection of personal data

During your visit, the Bank may collect some of your personal data such as:

- Basic identification information, such as your name, organization name, and contact details signature.
- Identification information (e.g., Company ID card/proof, and other national ID such as Aadhar number, Voter ID, PAN Card, proof of nationality as required.

- Electronic identification data (e.g. Laptop serial number, image recording such as CCTV).

Purpose of collection

Your personal data is collected to:

- To perform verification and validation of individuals (visitors) identity for entry gate pass.
- Ensure security and prevent loss, frauds, thefts within office premises .
- Comply with regulatory obligations mandated by relevant government authorities.
- Maintain operational records for audit and compliance purposes

Data Security

- We are committed to protecting your Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your Personal Data is executed with the third parties/ vendors/ service providers involved in providing services to us.
- The Bank has adopted ISO/IEC27001 standard, which is a globally accepted standard. The Bank's Datacentres, IT and Support functions are ISO 27001:2013 & ISO 27701:2022 certified.

Data retention

We make reasonable efforts to retain personal data only for so long as the information is necessary to comply with our obligations; and necessary to comply with legal, regulatory or internal policy requirements.

Your Data Principal Rights

We are committed to ensuring that you are aware of and can exercise your rights regarding your personal information.

Data principals have the following rights about their personal information:

- **Right of Access**: Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification**: Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure**: Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate**: Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights. When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights or any queries regarding your personal data you can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations.

Acknowledgement from Visitor

Visitors acknowledge that the collection, processing, and retention of their personal data shall be conducted in accordance with the terms set forth in this Privacy Notice and applicable data protection laws.

By providing personal information, visitors consent to its processing for legitimate purposes, including but not limited to employment administration, compliance obligations, security management, and workplace engagement initiatives.

Signature

Candidate Privacy Notice

Union Bank of India

Data Protection Office

1. Introduction

We, **Union Bank of India (hereafter referred to as "UBI", "we", "our")** are committed to protecting the privacy of individuals applying for employment with us. This notice explains how we process your personal data during and after the recruitment process. Protecting personal data is a core responsibility, and we have implemented robust physical, digital, and procedural safeguards to ensure its confidentiality.

Access to candidate personal data is strictly limited to authorized personnel. We recognize our duty to maintain the confidentiality of the personal data and sensitive information entrusted to us by the candidates and job seekers/ applicants.

The terms "**we**", "**us**", "**our**" & "**ours**" refer to UBI, and "**you**", "**your**" & "**yours**" refer to the candidate/ job seeker/ aspirant whose personal data is being referred to.

"Personal Data" means any data about an individual who is identifiable by or in relationship to such data.

"Sensitive Personal Data or Information" includes your and your dependents' personal data, but is not limited to,

- Passwords;
- Financial details such as bank account details, or tax information;
- Health-related information;
- Biometric data;
- Documentary data which are stored in paper (subsequently digitized) /electronic documents or copies of them such as Aadhaar/PAN/Voter ID/Driving License/Passport/CIBIL & other credit scores;

Any other information categorized as sensitive under applicable laws.

"Processing" means in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

2. Applicability

This notice applies to personal data collected from:

- Job applicants and prospective employees during recruitment and selection processes (whether full time or on contract basis, on internship or assignment to UBI).
- Information submitted via our career's portal, email, or physical forms.
- Data obtained through interviews, assessments, and background document verification.

3. What Personal Data We Collect & Process?

In the course of recruitment processes, our business operations, we may collect and process your personal data including but not limited to:

- Identification details (Name, Contact Information, Address).
- Professional details (Resume, CVs, Reference Letters, Education/ academic qualifications, Work Experience/ employment history and skills).
- Recruitment records (Interview evaluations, background verification reports).
- Recruitment-related information, such a citizenship, date of birth, residency, government issued identifiers, geographic location preferences, and remuneration details (where allowed), interactions over emails
- Information provided voluntarily during the hiring process
- Biometric Data
- CIBIL & other credit scores
- Images or videos are captured on CCTV for security purpose during visit to office for interviews.
- Special categories of personal data – We may capture the personal data relating to special category such as PWD for the purpose of recruitment, if applied by you under that category. However, we do not require the collection of health data documents for disabilities during the initial stages of the recruitment process. If you are offered a role, we may, where permitted by applicable law, request certain Sensitive Personal data and/or identification numbers to meet our legal and regulatory obligations.

  Depending on the stage of recruitment and in accordance with applicable laws, we may also conduct background checks. Such checks may involve information obtained from publicly available sources, previous employers or colleagues, educational institutions attended, credit reporting agencies, and criminal records databases.

4. Where do we obtain Personal Data from?

We collect personal data from multiple sources, such as:

- Directly from you (application forms, resumes, interviews etc).
- From recruitment agencies or referral programs.
- Through verification agencies for background checks.
- Digital platforms and other sources
- Police verification

5. Purpose for collecting and processing Personal Data

Personal Data means any data about an individual who is identifiable by or in relationship to such data

In accordance with applicable laws and regulations, the collection, storage, and processing of your personal data shall be carried out for legitimate business purposes, including but not limited to:

- Evaluating suitability for employment.
- Facilitate communication and providing response to your queries during the recruitment process
- Conducting interviews and assessments.
- Completing background checks and pre-employment verification.
- Complying with legal and regulatory requirements.

6. Sharing of Personal Data

We may share your data with following but not limited to:

- Background verification agencies.
- Recruitment partners.
- Legal or regulatory authorities when required.
- Any other third parties that are contractually obligated to implement appropriate data protection and confidentiality safeguards.

7. Use of Cookies

- We use cookies and similar technologies to enhance your browsing experience, analyse site traffic, and personalised content. Some cookies are essential for this site to function, while others help us understand your use and preferences enabling us to improve our services. These are stored locally on your computer or mobile devices. By clicking "Accept All", you consent to the storage of cookies on your device & its functionality. To customize your cookie preference, click “Customize” and select the categories you want to accept. You may choose to manage your preferences or modify/ withdraw your consent at any time by accessing cookie settings in your device.
- The Bank is not responsible for cookies placed in the device of user/s by any other website and Personal Data collected thereto. We do not control these cookies and once you have clicked on the advertisement and left the site, our Privacy Policy no longer applies.

8. Personal Data Security

- We are committed to protecting your Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your Personal Data is executed with the third parties/ vendors/ service providers involved in providing services to us.

- The Bank has adopted ISO/IEC27001 standards, which are globally accepted standards.
- The Bank's Datacentres, IT and Support functions are ISO 27001:2013 certified.

9. Data Principal Rights

Your rights regarding the processing of your personal data are important to us, and you can exercise these rights at any point.
You have certain Data Principal rights with respect to personal data belonging to you collected by UBI for the purposes mentioned in this Privacy Notice. The rights are available to you as per Digital Personal Data Protection Act, 2023 and/ or other applicable laws:

- **Right of Access:** Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification:** Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure:** Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate:** Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights. When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights, the data principal can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai: 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations

10. Withdrawal of Consent

Any individual has the right to withdraw their consent for the processing of their Personal Data at any time. Such withdrawal applies specifically to processing carried out for purposes such as marketing or promotional communications and will take effect only for future processing activities. It will not affect the lawfulness of any processing that was carried out prior to the withdrawal of consent. Even after consent is withdrawn, the Bank may continue to process

Personal Data where required to comply with legal or regulatory obligations, to protect the Bank’s lawful interests, to pursue available remedies, or to defend against existing or potential claims.
In accordance with the requirements of the Digital Personal Data Protection Act, 2023, a clear and accessible mechanism for withdrawal of consent is required. Data Principals may withdraw or modify their consent at any time through consent management option available on Union Bank of India’s website.

11. Retention of Personal Data

We may retain your Personal Data for as long as required for legitimate purposes that may include such as managing your contact and dealing with any concerns that may arise or otherwise if as may be required for any for legal, regulatory and/or statutory reasons.
If the Bank no more require to retain the information provided by the Employee, it will use best efforts to destroy or delete such employee Information as per our Bank’s internal policies.

Your personal data will be stored in accordance with applicable laws and kept as long as needed to carry out the purposes described in this Notice (or as otherwise required by applicable law). If you are successful with your job application, your personal data will be kept in accordance with our Employee Privacy Notice.

If you are unsuccessful with your job application, your personal data will be kept for the duration of the application process, plus a reasonable period of time after confirmation that your application was unsuccessful to allow us to record the reasons for our decision in relation to your application (including so that we can exercise, establish, or defend any legal claims).

12. Links to other Websites and Social Media

The Bank website may contain links to websites of other organizations that are not owned by Bank. This document does not cover how those organizations process your Personal Data. We encourage you to read the relevant privacy notice on the other websites that you may visit.
Please note that when visiting Bank’s official social media site/ page, you are subject to this document well as the social media platform's own terms and conditions.

13. Decision Making

Any decision made by us in relation to this document shall be at our sole discretion and the same shall be final and binding upon you.

14. Grievance Redressal

In case of any discrepancies or grievances, you may contact us at:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai: 400059

15. Notification of Changes

We reserve the right to amend, modify, vary, or update this Privacy Notice, at our sole discretion from time to time, as and when the need arises. You are encouraged to check our UBI career portal from time to time to stay informed of any changes. Except as otherwise stated in this Notice, any updates to this Notice will be effective from the date of publication on the career portal.

16. Acknowledgement from Candidate

Candidate acknowledges that the collection, processing, and retention of their personal data shall be conducted in accordance with the terms set forth in this Privacy Notice and applicable data protection laws.
By providing personal information, candidate consent to its processing for legitimate purposes, including but not limited to interview evaluation, background verification report.
By continuing employment, employees affirm their understanding of this Privacy Notice and agree to comply with organizational policies related to data protection and privacy.

Signature

This Privacy Notice was last updated on July 31, 2026.

Privacy Notice –
CASA Products and Term Deposits
Union Bank of India

Data Protection Office

1. Introduction

We, **Union Bank of India (hereinafter referred to as "the Bank" or "UBI")**, are committed to protecting the privacy of the Bank's customers' personal data and have taken all necessary measures to safeguard it. Keeping information secure is one of the banks most important responsibilities.

The Bank maintains **physical, electronic, and procedural safeguards** to protect customers' personal data. Access to such information is strictly limited to employees, **authorized service providers**, and other vendors for lawful purposes only. All employees and authorized service providers are bound by a **code of ethics** that mandates the confidential treatment of customer information, and any violation of this code is subject to disciplinary action.

The Bank shall not be held liable for disclosure of confidential information when such disclosure is:

- In accordance with this Privacy Notice,
- As per agreements with customers, or
- In compliance with applicable laws or directives from competent authorities.

The Bank recognizes and upholds the responsibility to maintain the confidentiality of all information entrusted to us by our customers.

Scope of this Privacy Notice

- This Privacy Notice ("document") applies when CASA (Current and Savings Account) product services or Term Deposit products of the Bank are availed, whether directly or through authorized channels, for any financial or non-financial transaction with the Bank.
- This Notice is framed to outline the Bank's broader commitment to maintaining high standards of privacy and responsible data handling. It sets forth the privacy practices followed by the Bank and the manner in which the Bank collects, uses, discloses, stores, secures, and disposes of Personal Data, whether processed in physical or electronic form. Further, this Policy also reflects the Bank's approach to meeting its obligations under applicable laws, including the Digital Personal Data Protection Act, 2023.
- Throughout this document, the terms **"we", "us", "our" & "ours"** refer to UBI, and the terms **"you", "your" & "yours"** refer to the individual whose personal data is being processed (e.g., customer, nominee, among others).

Definitions

Application: The Bank's mobile application or any other application through which the Bank's services can be availed electronically.

Personal Data: Any information relating to an individual that can identify such person directly or indirectly, in combination with other information available or likely to be available with the Bank.

Sensitive Personal Data: It is a subset of Personal Data. Wherever Sensitive Personal Data is not mentioned separately, it is deemed included under Personal Data.
Sensitive Personal Data or Information includes:

i. Financial information such as bank account, credit/debit card details, or other payment instrument details
ii. Physical, physiological, and mental health condition
iii. Medical records and history
iv. Biometric information
v. Password
vi. Any information received under the above clauses for processing, stored or processed under lawful contract, or including any other category which may fall under the ambit of Sensitive Personal Data (as defined by the Bank from time to time).

Website: A collection of publicly accessible, interlinked web pages of the Bank under a single domain name, created and maintained for various purposes.

2. Applicability

This is applicable to Personal Data and Sensitive Personal Data collected and processed by us or is received directly from you at our offices/branches or through the Bank's website, Application and electronic communications and any information collected by the Bank's server from the browser, or the physical forms that are later digitized.
Exceptions of Personal Data/Sensitive Personal Data-

i. Any information freely available in the public domain
ii. Any reviews, comments, messages, or blogs posted by customers on public sections of the Bank's website or application become published content and are not considered personal or sensitive data subject to this document.

3. What Personal Data does the Bank Collect & Process?

The Bank collects the following categories of Personal Data for providing CASA and term deposit-related services to you. Please note below is not an exhaustive list and may change as per the products and services offered to fulfil regulatory and legal requirements:

i. **Customer** - Name, first name, middle name, last name, date of birth, age, gender, marital status, nationality, religion, caste, contact details: address (home, permanent, residential), phone numbers, email IDs, depositor name, spouse's name, father's name, mother's maiden name, photograph, signature, CCTV footage, location data, identity and address proof: Aadhaar, PAN, passport, voter ID, CKYC number, NREGA job card, driving license, KYC documents, CIF ID, employment details, education qualification, Bank account details, account number, IFSC code, account statements, transaction history, card details (debit), payment instrument information

ii. **Nominee and beneficiary** - name, relationship, date of birth, address

4. Where does the bank obtain Personal Data from?

Most of the Personal Data processed by the Bank is provided directly by you through our website, mobile banking application, by visiting our branches, through our authorised third parties(such as business correspondents), or through Relationship Managers, and while using our products and services. We may also collect certain information through cookies when you visit our website. In addition, we may collect information about you from other sources as described below, and after verifying its authenticity, may add it to the data we already hold and process it in accordance with this Privacy Policy.
If Personal Data is collected from third-party service providers for the purpose of offering relevant marketing content, offers, or services, such data will be used and processed only with your consent. These third-party service providers may include email service providers, and other authorised entities as appropriate.

5. Purpose for collecting and processing Personal Data

The Bank processes your Personal Data for the following purposes:

➢ Provide products and assist in and administer the provision of services to you, which includes activities like account opening, onboarding, and service facilitation:

- To process account opening (in person, branch-assisted, VKYC)
- To issue and deliver debit cards
- To facilitate Aadhaar Verification via UIDAI
- To onboard clients and partners for banking and financial services
- To facilitate NEFT transactions, NACH mandates, and digital/physical payments
- To manage locker facilities and cheque books
- To deliver services via call centre and doorstep banking
- To maintain records and reconcile accounts
- To calculate, accrue, and credit interest on savings accounts and term deposits.
- To process creation, renewal, premature withdrawal, or closure of term deposits.
- To generate and maintain deposit receipts, maturity instructions and renewal mandates.
- To deduct and report TDS on interest income as required under applicable tax laws.
- To provide financial literacy training and general services
- To generate financial statements
- To provide general banking services

➢ Prevent, detect, investigate and prosecute fraud and alleged fraud, money laundering and other crimes and to verify your identity which includes KYC, compliance, and fraud related activities:

- Includes KYC, compliance, and fraud-related activities:
- To verify and update customer contact details

- To conduct due diligence and investigations
- To fulfil legal obligations and provide data to auditors
- To facilitate Re-KYC and investigate staff accountability

➢ Providing information about products, offers, promotions, and services, which includes marketing and outreach activities in accordance with the consent provided by you.

➢ Process and deal with any complaints or enquiries made by or about you, which includes grievance redressal and customer support:

- To handle customer complaints and RCA
- To resolve GST-related complaints
- To investigate and redress grievances

➢ To analyse your Personal Data for Anti-Money Laundering (AML) and other regulatory compliance requirements, provisioning of services, and for other legitimate business purposes necessary to support the Bank's operations.

➢ For reporting to regulatory authorities and internal audits.

6. Sharing of Personal Data

The Bank may disclose your Personal Data to various categories of third parties after obtaining your consent for the same or as part of legitimate use as per DPDPA. However, the Bank may also disclose your Personal Data without your consent where such disclosure is required under applicable laws, where the Bank is mandated to cooperate with statutory, regulatory, or governmental authorities, or where such disclosure is necessary for the legitimate use under the DPDP Act. The third parties include:

i. **Other Group Companies, Partners, and Subsidiaries** for providing or enhancing products, services, and customer experience.

ii. **Sub-contractors, agents, or service providers** who work for the Bank or provide services/products on behalf of the Bank.

iii. **Agents or service providers** engaged for activities connected to customer servicing, operational support, marketing (where permissible), or other contractual obligations.

iv. **Law enforcement agencies**, **government authorities**, Income Tax Authorities, **investigating agencies**, and any authority empowered under law.

v. **Regulators**, including the **Reserve Bank of India**, Indian or overseas regulatory bodies, auditors, and entities appointed by regulators to conduct inspections, audits, or investigations.

vi. **Courts, tribunals, judicial or quasi-judicial bodies**, arbitrators, and arbitration tribunals.

vii. Situations involving **regulatory reporting**, compliance with legal processes, or to **assert or defend the Bank's legal rights and interests**.

7. Withdrawal of Consent

Any individual has the right to withdraw their consent for the processing of their Personal Data at any time. Such withdrawal applies specifically to processing carried out for purposes such as marketing or promotional communications and will take effect only for future processing activities. It will not affect the lawfulness of any processing that was carried out prior to the withdrawal of consent. Even after consent is withdrawn, the Bank may continue to process Personal Data where required to comply with legal or regulatory obligations, to protect the Bank's lawful interests, to pursue available remedies, or to defend against existing or potential claims.

In accordance with the requirements of the Digital Personal Data Protection Act, 2023, a clear and accessible mechanism for withdrawal of consent is required. Data Principals may withdraw or modify their consent at any time by using the consent management option available on the corporate website, internet banking portal, mobile banking application, among others.

8. Processing of Personal Data of Children and Persons with Disability

We obtain verifiable consent from a parent or lawful guardian before processing the Personal Data of minors. We ensure that such processing does not have any detrimental effect on the child's well-being. The Bank does not engage in profiling, behavioural monitoring, or targeted advertising directed at children, and their data is not used for marketing or promotional activities. In line with the principle of data minimisation, only essential information required for providing the requested services is collected.

Where the individual is a Person with Disability who is unable to provide legally valid consent, we obtain verifiable consent from the lawful guardian before processing their Personal Data. Such processing is carried out with due care to ensure that it does not adversely impact the individual's well-being.

9. Use of Cookies

- We use cookies and similar technologies to enhance your browsing experience, analyse site traffic, and personalised content. Some cookies are essential for this site to function, while others help us understand your use and preferences enabling us to improve our services. These are stored locally on your computer or mobile devices. By clicking "Accept All", you consent to the storage of cookies on your device & its functionality. To customize your cookie preference, click "Customize" and select the categories you want to accept. You may choose to manage your preferences or modify/ withdraw your consent at any time by accessing cookie settings in your device.
- The Bank is not responsible for cookies placed in the device of user/s by any other website and Personal Data collected thereto. We do not control these cookies and once you have clicked on the advertisement and left the site, our Privacy Policy no longer applies.

10. Personal Data Security

- The Bank is committed to protecting your Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your Personal Data is executed with the third parties/ vendors/ service providers involved in providing services to us.
- The Bank has adopted ISO/IEC 27001 standards, which are globally accepted standards. The Bank's Data centres, IT and Support functions are ISO 27001:2013 certified.

11. Data Principal Rights

We are committed to ensuring that you are aware of and can exercise your rights regarding your personal Data

Data principals have the following rights about their personal Data:

- **Right of Access**: Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification**: Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure**: Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate**: Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights. When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights, customer can visit corporate website, internet banking portal, mobile banking application, among others and can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations.

12. Retention of Personal Data

The Bank may retain your Personal Data for as long as required for legitimate purposes that may include such as managing your account and dealing with any concerns that may arise or otherwise if as may be required for any for legal, regulatory and/or statutory reasons.

If the Bank no longer requires the retention of the information provided by the Customer, it will use best efforts to destroy or delete such Customer Information as per our Bank's internal policies.

13. Links to other Websites and Social Media

The Bank website may contain links to websites of other organizations that are not owned by Bank. This document does not cover how those organizations process your Personal Data. We encourage you to read the relevant privacy notice on the other websites that you may visit.

Please note that when visiting Bank's official social media site/ page, you are subject to this document well as the social media platform's own terms and conditions.

14. Conflict of Laws & Disputes

You agree that, irrespective of your location or country of jurisdiction, this document and its contents shall be subject to and governed by Indian laws (as amended from time to time) as may be applicable and that you waive all your rights which you may have in relation to this document under any contract or relevant laws applicable to the jurisdiction where you are situated and/or by which you are governed.

Any disputes over inter alia collection, storage and handling of Personal Data will be governed by this document, Terms and Conditions and by the laws of India and courts of India shall have exclusive jurisdiction.

15. Grievance Redressal

In case of any discrepancies or grievances, you may contact us at

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

16. Notification of Changes

We may update this Privacy Policy from time to time to reflect changes in our business, technology, or legal requirements. We encourage you to review this Privacy Policy regularly to stay informed about our privacy practices and any changes we may make.

This Privacy Notice was last updated on July 31, 2026.

Privacy Notice -

Retail Loans

Union Bank of India

Data Protection Office

1. Introduction

We, **Union Bank of India (hereinafter referred to as "the Bank" or "UBI")**, are committed to protecting the privacy of the Bank's customers' personal data and have taken all necessary measures to safeguard it. Keeping information secure is one of the bank's most important responsibilities.

The Bank maintains **physical, electronic, and procedural safeguards** to protect customers' personal data. Access to such information is strictly limited to employees, **authorized service providers**, and other vendors for lawful purposes only. All employees and authorized service providers are bound by a **code of ethics** that mandates the confidential treatment of customer information, and any violation of this code is subject to disciplinary action.

The Bank shall not be held liable for disclosure of confidential information when such disclosure is:

- In accordance with this Privacy Notice,
- As per agreements with customers, or
- In compliance with applicable laws or directives from competent authorities.

The Bank recognizes and upholds the responsibility to maintain the confidentiality of all information entrusted to us by our customers.

Scope of this Privacy Notice

- This Privacy Notice ("document") applies when any loan product or credit facility of the Bank is availed, whether directly or through authorised channels, for any financial or non-financial transaction with the Bank.
- This Notice is framed to outline the Bank's broader commitment to maintaining high standards of privacy and responsible data handling. It sets forth the privacy practices followed by the Bank and the manner in which the Bank collects, uses, discloses, stores, secures, and disposes of Personal Data, whether processed in physical or electronic form. Further, this Policy also reflects the Bank's approach to meeting its obligations under applicable laws, including the Digital Personal Data Protection Act, 2023.
- Throughout this document, the terms **"we", "us", "our" & "ours"** refer to UBI, and the terms **"you", "your" & "yours"** refer to the individual whose personal data is being processed (e.g., customer, guarantor, builder, seller, vehicle owner, among others).

Definitions

Application: The Bank's mobile application or any other application through which the Bank's services can be availed electronically.

Personal Data: Any information relating to an individual that can identify such person directly or indirectly, in combination with other information available or likely to be available with the Bank.

Sensitive Personal Data: It is a subset of Personal Data. Wherever Sensitive Personal Data is not mentioned separately, it is deemed included under Personal Data.
Sensitive Personal Data or Information includes:

1. Financial information such as bank account, credit/debit card details, or other payment instrument details
2. Physical, physiological, and mental health conditions
3. Medical records and history
4. Biometric information
5. Password
6. Any information received under the above clauses for processing, stored or processed under a lawful contract, or including any other category which may fall under the ambit of Sensitive Personal Data (as defined by the Bank from time to time).

Website: A collection of publicly accessible, interlinked web pages of the Bank under a single domain name, created and maintained for various purposes.

2. Applicability

This is applicable to Personal Data and Sensitive Personal Data collected and processed by us or is received directly from you at our offices/branches or through the Bank's website, Application and electronic communications, and any information collected by the Bank's server from the browser, or the physical forms that are later digitized.
Exceptions of Personal Data/Sensitive Personal Data-

- Any information freely available in the public domain
- Any reviews, comments, messages, or blogs posted by customers on public sections of the Bank's website or application become published content and are not considered personal or sensitive data subject to this document.

3. What Personal Data does the Bank Collect & Process?

The Bank collects the following categories of Personal Data for providing services to you. Please note below is not an exhaustive list and may change as per the products and services offered to fulfil regulatory and legal requirements:

i. **Customer -** Name, first name, middle name, last name, date of birth, age, gender, marital status, nationality, religion, caste, contact details: address (home, permanent, residential), phone numbers, email IDs, depositor name, spouse's name, father's name, mother's maiden name, photograph, signature, CCTV footage, location data, identity and address proof: Aadhaar, PAN, passport, voter ID, CKYC number, driving license, KYC documents, CIF ID, employment details, education qualification, Bank account details, account number, IFSC code, account statements, transaction history, Annual income, salary slips, income tax returns (Form 16), Loan details: amount, sanction date, Credit score (e.g., CIBIL), net worth statements

ii. **Guarantor -** Name, first name, middle name, last name, date of birth, age, gender, marital status, nationality, religion, caste, contact details: address (home, permanent, residential), phone numbers, email IDs, depositor name, spouse's name, father's name, mother's maiden name, photograph, signature, CCTV footage, location data, identity and address proof: Aadhaar, PAN, passport, voter ID, driving license, KYC documents, CIF ID, employment details, education qualification, Bank account details, account number, IFSC code, account statements, transaction history, payment instrument information, Annual income, salary slips, income tax returns (Form 16), Loan details: amount, sanction date, Credit score (e.g., CIBIL), net worth statements

iii. **Property Owner -** Name, Address, Mobile Number

iv. **Builder-** Name

v. **Reference -** Name, Address, Email, Mobile Number

vi. **Seller** – Name, Address, Mobile Number, Aadhaar, PAN

vii. **Previous Vehicle Owner -** Name, Address, Mobile Number

viii. **Dealer-** Name, Address, Mobile Number, Email ID, Bank Account number

4. Where does the bank obtain Personal Data from?

Most of the Personal Data processed by the Bank is provided directly by you through our website, mobile banking application, by visiting our branches, through our authorised third parties (such as DSAs, dealers, and CSAs), or through Relationship Managers, Marketing Officers, and while using our products and services. We may also collect certain information through cookies when you visit our website. In addition, we may collect information about you from other sources as described below, and after verifying its authenticity, may add it to the data we already hold and process it in accordance with this Privacy Policy.
If Personal Data is collected from third-party service providers for the purpose of offering relevant marketing content, offers, or services, such data will be used and processed only with your consent. These third-party service providers may include email service providers and other authorised entities as appropriate.

5. Purpose for collecting and processing Personal Data

The Bank processes your Personal Data for the following purposes:

➢ Provide loan products and assist in administering related services to you, which include activities like account opening, product delivery, onboarding, and service facilitation:

- To process account opening (in person, branch-assisted, VKYC)
- UIDAI Aadhaar Verification
- To set up NACH mandates for EMI repayment if applicable.
- To monitor loan account performance
- To maintain records and reconcile accounts
- To evaluate and onboard loan accounts from NBFCs
- To facilitate joint loan disbursement

- To contact customers for EMI reminders
- To assess loan eligibility and creditworthiness
- To verify income, employment, business financials
- To verify collateral documents (property, gold, vehicle etc.)
- To generate financial statements and maintain borrower accounts
- To provide general banking services
- To conduct property valuation, technical verification, legal scrutiny, and title verification for secured loans.
- To issue notices for overdue payments

➢ Prevent, detect, investigate and prosecute fraud and alleged fraud, money laundering and other crimes and to verify your identity which includes KYC, compliance, and fraud related activities:

- To verify and update customer contact details
- To conduct due diligence and investigations
- To engage recovery agencies (as permitted by RBI)
- To report wilful defaulters, fraud accounts, and other classifications to regulatory authorities as required under applicable laws.
- To fulfil legal obligations and provide data to auditors
- To facilitate Re-KYC and investigate staff accountability
- To monitor and manage stressed loan accounts
- To identify early signs of financial distress
- To comply with SARFAESI, RBI guidelines, FIU reporting

➢ Providing information about products, offers, promotions, and services, which includes marketing and outreach activities in accordance with the consent provided by you.

➢ Process and deal with any complaints or enquiries made by or about you which includes grievance redressal and customer support:

- To handle customer complaints and RCA
- To recover the dues
- To resolve GST-related complaints
- To investigate and redress grievances
- To reach out to customers to recover the loans
- To ensure secure and efficient recovery of dues

➢ To analyse your Personal Data for Anti-Money Laundering (AML) and other regulatory compliance requirements, provisioning of services, assessing loan and credit eligibility, and for other legitimate business purposes necessary to support the Bank’s operations.

➢ For reporting to regulatory authorities and internal audits

6. Sharing of Personal Data

The Bank may disclose your Personal Data to various categories of third parties after obtaining your consent for the same or as part of legitimate use as per DPDPA. However, the Bank may also disclose your Personal Data without your consent where such disclosure is required under applicable laws, where the Bank is mandated to cooperate with statutory, regulatory, or governmental authorities, or where such disclosure is necessary for the legitimate use under the DPDP Act. The third parties include:

i. Other Group Companies, Partners, and Subsidiaries for providing or enhancing products, services, and customer experience.
ii. Sub-contractors, agents, or service providers who work for the Bank or provide services/products on behalf of the Bank.
iii. Partners offering co-branded services, products, or programs, where such sharing is necessary to deliver the offering.
iv. Agents or service providers engaged for activities connected to customer servicing, operational support, marketing (where permissible), or other contractual obligations.
v. Law enforcement agencies, government authorities, investigating agencies, and any authority empowered under law.
vi. Regulators, including the Reserve Bank of India, Indian or overseas regulatory bodies, auditors, and entities appointed by regulators to conduct inspections, audits, or investigations.
vii. Empanelled valuers, lawyers, appraisers, or authorised service providers/agents engaged for valuation, legal scrutiny, verification, and recovery actions in the event of default.
viii. Courts, tribunals, judicial or quasi-judicial bodies, arbitrators, and arbitration tribunals.
ix. Credit information companies/credit bureaus, statutory bodies, and any persons or entities to whom disclosure is mandatory under applicable laws.
x. Situations involving regulatory reporting, compliance with legal processes, or to assert or defend the Bank's legal rights and interests.

7. Withdrawal of Consent

Any individual has the right to withdraw their consent for the processing of their Personal Data at any time. Such withdrawal applies specifically to processing carried out for purposes such as marketing or promotional communications and will take effect only for future processing activities. It will not affect the lawfulness of any processing that was carried out prior to the withdrawal of consent. Even after consent is withdrawn, the Bank may continue to process Personal Data where required to comply with legal or regulatory obligations, to protect the Bank's lawful interests, to pursue available remedies, or to defend against existing or potential claims.

In accordance with the requirements of the Digital Personal Data Protection Act, 2023, a clear and accessible mechanism for withdrawal of consent is required. Data Principals may withdraw or modify their consent at any time by using the consent management option available on the corporate website, internet banking portal, mobile banking application, among others.

8. Processing of Personal Data of Children and Persons with Disability

We obtain verifiable consent from a parent or lawful guardian before processing the Personal Data of minors. We ensure that such processing does not have any detrimental effect on the child’s well-being. The Bank does not engage in profiling, behavioural monitoring, or targeted advertising directed at children, and their data is not used for marketing or promotional activities. In line with the principle of data minimisation, only essential information required for providing the requested services is collected.
Where the individual is a Person with Disability who is unable to provide legally valid consent, we obtain verifiable consent from the lawful guardian before processing their Personal Data. Such processing is carried out with due care to ensure that it does not adversely impact the individual’s well-being.

9. Use of Cookies

- We use cookies and similar technologies to enhance your browsing experience, analyse site traffic, and personalize content. Some cookies are essential for this site to function, while others help us understand your use and preferences, enabling us to improve our services. These are stored locally on your computer or mobile devices. By clicking "Accept All", you consent to the storage of cookies on your device & its functionality. To customize your cookie preference, click “Customize” and select the categories you want to accept. You may choose to manage your preferences or modify/ withdraw your consent at any time by accessing cookie settings in your device.
- The Bank is not responsible for cookies placed in the device of user/s by any other website and Personal Data collected thereto. We do not control these cookies and once you have clicked on the advertisement and left the site, our Privacy Policy no longer applies.

10. Personal Data Security

- The Bank is committed to protecting your Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your Personal Data are executed with the third parties/ vendors/ service providers involved in providing services to us.
- The Bank has adopted ISO/IEC 27001 standards, which are globally accepted standards. The Bank’s Datacentres, IT and Support functions are ISO 27001:2013 certified.

11. Data Principal Rights

We are committed to ensuring that you are aware of and can exercise your rights regarding your personal data.

Data principals have the following rights about their personal Data:

- **Right of Access**: Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification**: Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure**: Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate**: Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights. When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights, customer can visit corporate website, internet banking portal, mobile banking application, among others and can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations.

12. Retention of Personal Data

The Bank may retain your Personal Data for as long as required for legitimate purposes that may include managing your account and dealing with any concerns that may arise or otherwise if as may be required for any for legal, regulatory and/or statutory reasons.

If the Bank no longer requires the retention of the information provided by the Customer, it will use best efforts to destroy or delete such Customer Information as per our Bank's internal policies.

13. Links to other Websites and Social Media

The Bank website may contain links to websites of other organizations that are not owned by Bank. This document does not cover how those organizations process your Personal Data. We encourage you to read the relevant privacy notice on the other websites that you may visit.

Please note that when visiting Bank's official social media site/ page, you are subject to this document well as the social media platform's own terms and conditions.

14. Conflict of Laws & Disputes

You agree that, irrespective of your location or country of jurisdiction, this document and its contents shall be subject to and governed by Indian laws (as amended from time to time) as may be applicable and that you waive all your rights which you may have in relation to this document under any contract or relevant laws applicable to the jurisdiction where you are situated and/or by which you are governed.

Any disputes over inter alia collection, storage and handling of Personal Data will be governed by this document, Terms and Conditions and by the laws of India and courts of India shall have exclusive jurisdiction.

15. Grievance Redressal

In case of any discrepancies or grievances, you may contact us at

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

16. Notification of Changes

We may update this Privacy Policy from time to time to reflect changes in our business, technology, or legal requirements. We encourage you to review this Privacy Policy regularly to stay informed about our privacy practices and any changes we may make.

This Privacy Notice was last updated on July 31, 2026.

Privacy Notice – Credit Cards

Union Bank of India

Data Protection Office

1. Introduction

We, **Union Bank of India (hereinafter referred to as "the Bank" or "UBI")**, are committed to protecting the privacy of the Bank's customers' personal data and have taken all necessary measures to safeguard it. Keeping information secure is one of the banks most important responsibilities.

The Bank maintains **physical, electronic, and procedural safeguards** to protect customers' personal data. Access to such information is strictly limited to employees, **authorized service providers**, and other vendors for lawful purposes only. All employees and authorized service providers are bound by a **code of ethics** that mandates the confidential treatment of customer information, and any violation of this code is subject to disciplinary action.

The Bank shall not be held liable for disclosure of confidential information when such disclosure is:

- In accordance with this Privacy Notice,
- As per agreements with customers, or
- In compliance with applicable laws or directives from competent authorities.

The Bank recognizes and upholds the responsibility to maintain the confidentiality of all information entrusted to us by our customers.

Scope of this Privacy Notice

- This Privacy Notice ("document") applies to customers who apply for, hold, or use credit card products and related services offered by the Bank, whether the services are availed directly from the Bank or through authorized merchant or service partners. The personal data of Data Principals including but not limited to card holders, joint card holders, nominees, parents, guardians and/ or spouse may be processed for the purpose of provisioning of these services.
- This Notice is framed to outline the Bank's broader commitment to maintaining high standards of privacy and responsible data handling of personal data in relation to credit card services. It sets forth the privacy practices followed by the Bank and the manner in which the Bank collects, uses, discloses, stores, secures, and disposes of Personal Data, whether processed in physical or electronic form. Further, this Policy also reflects the Bank's approach to meeting its obligations under applicable laws, including the Digital Personal Data Protection Act, 2023.
- Throughout this document, the terms **"we", "us", "our" & "ours"** refer to UBI, and the terms **"you", "your" & "yours"** refer to the individual whose personal data is being processed.

Definitions

Application: The Bank's mobile application or any other application through which the Bank's services can be availed electronically.

Personal Data: Any information relating to an individual that can identify such person directly or indirectly, in combination with other information available or likely to be available with the Bank.

Sensitive Personal Data: It is a subset of Personal Data. Wherever Sensitive Personal Data is not mentioned separately, it is deemed included under Personal Data.

Sensitive Personal Data or Information includes:

i. Financial information such as bank account, credit/debit card details, or other payment instrument details
ii. Physical, physiological, and mental health condition
iii. Medical records and history
iv. Biometric information
v. Password
vi. Any information received under the above clauses for processing, stored or processed under lawful contract or including any other category which may fall under the ambit of Sensitive Personal Data (as defined by the Bank from time to time).

Website: A collection of publicly accessible, interlinked web pages of the Bank under a single domain name, created and maintained for various purposes.

2. Applicability

This is applicable to Personal Data and Sensitive Personal Data collected and processed by us or is received directly from you at our offices/branches or through the Bank's website, Application and electronic communications and any information collected by the Bank's server from the browser, or the physical forms that are later digitized.

Exceptions of Personal Data/Sensitive Personal Data-

- Any information freely available in the public domain.
- Any reviews, comments, messages, or blogs posted by customers on public sections of the Bank's website or application become published content and are not considered personal or sensitive data subject to this document.

3. What Personal Data does the Bank Collect & Process?

The Bank collects and processes the following categories of Personal Data for providing credit card products and related services. This list is indicative and not exhaustive and may be updated based on the nature of products, services, regulatory requirements, or applicable laws.

i. **Customer** - full name (first name, middle name, last name), date of birth, age, gender, marital status, permanent address, mailing/residential address, office address, mobile number, and email ID, photograph, signature, PAN, Aadhaar, passport, voter ID, driving licence, other KYC documents, CIF ID (for UBI account holders), employment details, occupation, employer name, educational qualifications, income details such as annual income, salary slips, income tax returns, Form 16, details of existing credit cards, including issuing bank name, credit limit, and card number.

ii. **Nominee -** name, age, email ID, contact number, guardian name (in case of minor), signature.

iii. **Joint card holder -** full name (first name, middle name, last name), relationship, gender, marital status, mobile number, email ID, date of birth, photograph, identification documents (Voter ID, Driving License, Passport, Aadhaar, PAN).

4. Where does the bank obtain Personal Data from?

Most of the personal data processed by the Bank is provided directly by you through our website, by visiting our branches, through our authorized third parties (such as DSAs and CSAs), through Relationship Managers, or while availing and using our products and services. We may also collect certain information through cookies when you visit our website. In addition, we may collect information about you from other sources as described below, and after verifying its authenticity, may add it to the data we already hold and process it in accordance with this Privacy Policy.

Where personal data is obtained from third-party service providers for the purpose of offering relevant products, marketing content, offers, or services, such processing will be carried out only with your consent, wherever required. These third parties may include email service providers, other card issuers, credit information companies (such as CIBIL), financial institutions, subsidiaries, affiliates or associates of UBI, and authorized partners involved in activities such as co-branding, reward redemption, and printing and dispatch of credit cards.

5. Purpose for collecting and processing Personal Data

The Bank processes your Personal Data for the following purposes:

➢ Provide credit card products and assist in and administer the provision of services to you, which includes activities like credit card account opening, credit card delivery, customer onboarding, and service facilitation:

- To onboard the customer and process credit card applications.
- To assess eligibility, including income, creditworthiness, and other applicable criteria.
- To conduct Aadhaar Verification.
- To capture, verify, and maintain nominee details where applicable.
- To obtain and verify credit information from CIBIL or other credit information bureaus.
- To conduct customer due diligence and risk profiling in line with regulatory requirements.
- To create, issue, manage, and service the credit card account.
- To maintain records and reconcile accounts.
- To provide and manage insurance or protection benefits linked to the credit card.

- To suspend or prematurely close the credit card account in accordance with applicable terms, conditions, and regulatory requirements.
- To provide general banking services.

➢ Prevent, detect, investigate and prosecute fraud and alleged fraud, money laundering and other crimes and to verify your identity which includes KYC, compliance, and fraud related activities:

- To verify and update customer contact details.
- To conduct due diligence and investigations.
- To fulfil legal obligations and provide data to auditors.
- To facilitate Re-KYC and investigate staff accountability.
- To monitor transactions and comply with regulatory reporting obligations.
- To monitor and manage stressed loan accounts.
- To identify early signs of financial distress.

➢ Providing information about products, offers, promotions, and services, which includes marketing and outreach activities in accordance with the consent provided by you.

➢ Process and deal with any complaints or enquiries made by or about you which includes grievance redressal and customer support:

- To handle customer complaints and RCA.
- To reach out to customers to recover the dues.
- To recover the dues and manage the defaults.
- To investigate and redress grievances.

➢ To analyse your Personal Data for Anti-Money Laundering (AML) and other regulatory compliance requirements, provisioning of services, assessing loan and credit eligibility, and for other legitimate business purposes necessary to support the Bank's operations.

➢ For reporting to regulatory authorities and internal audits.

6. Sharing of Personal Data

The Bank may disclose your Personal Data to various categories of third parties after obtaining your consent for the same or as part of legitimate use as per DPDPA. However, the Bank may also disclose your Personal Data without your consent where such disclosure is required under applicable laws, where the Bank is mandated to cooperate with statutory, regulatory, or governmental authorities, or where such disclosure is necessary for the legitimate use under the DPDP Act. The third parties include:

i. **Other Group Companies, Partners, and Subsidiaries** for providing or enhancing products, services, and customer experience.

ii. **Sub-contractors, agents, or service providers** who work for the Bank or provide services/products on behalf of the Bank.

iii. **Partners offering co-branded services, products, or programs**, where such sharing is necessary to deliver the offering.

iv. **Agents or service providers** engaged for activities connected to customer servicing, operational support, marketing (where permissible), or other contractual obligations.

v. **Law enforcement agencies**, **government authorities**, **investigating agencies**, and any authority empowered under law.

vi. **Regulators**, including the **Reserve Bank of India**, Indian or overseas regulatory bodies, auditors, and entities appointed by regulators to conduct inspections, audits, or investigations.

vii. **Courts, tribunals, judicial or quasi-judicial bodies**, arbitrators, and arbitration tribunals.

viii. **Credit information companies / credit bureaus**, statutory bodies, and any persons or entities to whom disclosure is mandatory under applicable laws.

ix. Situations involving **regulatory reporting**, compliance with legal processes, or to **assert or defend the Bank's legal rights and interests**.

7. Withdrawal of Consent

Any individual has the right to withdraw their consent for the processing of their Personal Data at any time. Such withdrawal applies specifically to processing carried out for purposes, such as marketing or promotional communications, and will take effect only for future processing activities. It will not affect the lawfulness of any processing that was carried out prior to the withdrawal of consent. Even after consent is withdrawn, the Bank may continue to process Personal Data where required to comply with legal or regulatory obligations, to protect the Bank's lawful interests, to pursue available remedies, or to defend against existing or potential claims.

In accordance with the requirements of the Digital Personal Data Protection Act, 2023, a clear and accessible mechanism for withdrawal of consent is required. Data Principals may withdraw or modify their consent at any time by using the consent management option available on the corporate website, internet banking portal, mobile banking application, among others.

8. Processing of Personal Data of Children and Persons with Disability

We obtain verifiable consent from a parent or lawful guardian before processing the Personal Data of minors. We ensure that such processing does not have any detrimental effect on the child's well-being. The Bank does not engage in profiling, behavioural monitoring, or targeted advertising directed at children, and their data is not used for marketing or promotional activities. In line with the principle of data minimisation, only essential information required for providing the requested services is collected.

Where the individual is a Person with Disability who is unable to provide legally valid consent, we obtain verifiable consent from the lawful guardian before processing their Personal Data. Such processing is carried out with due care to ensure that it does not adversely impact the individual's well-being.

9. Use of Cookies

- We use cookies and similar technologies to enhance your browsing experience, analyse site traffic, and personalised content. Some cookies are essential for this site to function, while others help us understand your use and preferences enabling us to improve our services. These are stored locally on your computer or mobile devices. By clicking "Accept All", you consent to the storage of cookies on your device & its functionality. To customize your cookie preference, click "Customize" and select the categories you want to accept. You may choose to manage your preferences or modify/ withdraw your consent at any time by accessing cookie settings in your device.
- The Bank is not responsible for cookies placed in the device of user/s by any other website and Personal Data collected thereto. We do not control these cookies and once you have clicked on the advertisement and left the site, our Privacy Policy no longer applies.

10. Personal Data Security

- The Bank is committed to protecting your Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your Personal Data is executed with the third parties/ vendors/ service providers involved in providing services to us.
- The Bank has adopted ISO/IEC 27001 standards, which are globally accepted standards. The Bank's Datacentres, IT and Support functions are ISO 27001:2013 certified.

11. Data Principal Rights

We are committed to ensuring that you are aware of and can exercise your rights regarding your personal data.

Data principals have the following rights about their personal Data:

- **Right of Access**: Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification**: Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure**: Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate**: Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights.

When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights, customer can visit corporate website, internet banking portal, mobile banking application, among others and can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations.

12. Retention of Personal Data

The Bank may retain your Personal Data for as long as required for legitimate purposes that may include such as managing your account and dealing with any concerns that may arise or otherwise if as may be required for any for legal, regulatory and/or statutory reasons.

If the Bank no longer requires the retention of the information provided by the Customer, it will use best efforts to destroy or delete such Customer Information as per our Bank's internal policies.

13. Links to other Websites and Social Media

The Bank website may contain links to websites of other organizations that are not owned by Bank. This document does not cover how those organizations process your Personal Data. We encourage you to read the relevant privacy notice on the other websites that you may visit.

Please note that when visiting Bank's official social media site/ page, you are subject to this document well as the social media platform's own terms and conditions.

14. Conflict of Laws & Disputes

You agree that, irrespective of your location or country of jurisdiction, this document and its contents shall be subject to and governed by Indian laws (as amended from time to time) as may be applicable and that you waive all your rights which you may have in relation to this document under any contract or relevant laws applicable to the jurisdiction where you are situated and/or by which you are governed.

Any disputes over inter alia collection, storage and handling of Personal Data will be governed by this document, Terms and Conditions and by the laws of India and courts of India shall have exclusive jurisdiction.

15. Grievance Redressal

In case of any discrepancies or grievances, you may contact us at

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

16. Notification of Changes

We may update this Privacy Policy from time to time to reflect changes in our business, technology, or legal requirements. We encourage you to review this Privacy Policy regularly to stay informed about our privacy practices and any changes we may make.

This Privacy Notice was last updated on July 31, 2026.

Privacy Notice – Wholesale Banking

Union Bank of India

Data Protection Office

1. Introduction

We, **Union Bank of India (hereinafter referred to as "the Bank" or "UBI")**, are committed to protecting the privacy of the Bank's customers' personal data and have taken all necessary measures to safeguard it. Keeping information secure is one of the banks most important responsibilities.

The Bank maintains **physical, electronic, and procedural safeguards** to protect customers' personal data. Access to such information is strictly limited to employees, **authorized service providers**, and other vendors for lawful purposes only. All employees and authorized service providers are bound by a **code of ethics** that mandates the confidential treatment of customer information, and any violation of this code is subject to disciplinary action.

The Bank shall not be held liable for disclosure of confidential information when such disclosure is:

- In accordance with this Privacy Notice,
- As per agreements with customers, or
- In compliance with applicable laws or directives from competent authorities.

The Bank recognizes and upholds the responsibility to maintain the confidentiality of all information entrusted to us by our customers.

Scope of this Privacy Notice

- This Privacy Notice ("document") applies to Data Principals who apply for, avail or are currently availing wholesale banking products such as MSME loans and related services offered by the Bank, whether the services are availed directly from the Bank or through authorized merchant or service partners. The personal data of Data Principals including but not limited to promoters, partners, proprietors, directors, guarantors, father and/ or spouse may be processed for the purpose of provisioning of these services.
- This Notice is framed to outline the Bank's broader commitment to maintaining high standards of privacy and responsible data handling of personal data in relation to wholesale banking products and services such as MSME loans. It sets forth the privacy practices followed by the Bank and the manner in which the Bank collects, uses, discloses, stores, secures, and disposes of Personal Data, whether processed in physical or electronic form. Further, this Policy also reflects the Bank's approach to meeting its obligations under applicable laws, including the Digital Personal Data Protection Act, 2023.
- Throughout this document, the terms **"we", "us", "our" & "ours"** refer to UBI, and the terms **"you", "your" & "yours"** refer to the individual whose personal data is being processed.

Definitions

Application: The Bank's mobile application or any other application through which the Bank's services can be availed electronically.

Personal Data: Any information relating to an individual that can identify such person directly or indirectly, in combination with other information available or likely to be available with the Bank.

Sensitive Personal Data: It is a subset of Personal Data. Wherever Sensitive Personal Data is not mentioned separately, it is deemed included under Personal Data.
Sensitive Personal Data or Information includes:

- Financial information such as bank account, credit/debit card details, or other payment instrument details
- Physical, physiological, and mental health condition
- Medical records and history
- Biometric information
- Password
- Any information received under the above clauses for processing, stored or processed under lawful contract including any other category which may fall under the ambit of Sensitive Personal Data (as defined by the Bank from time to time).

Website: A collection of publicly accessible, interlinked web pages of the Bank under a single domain name, created and maintained for various purposes.

2. Applicability

This is applicable to Personal Data and Sensitive Personal Data collected and processed by us or is received directly from you at our offices/branches or through the Bank's website, Application and electronic communications and any information collected by the Bank's server from the browser, or the physical forms that are later digitized.
Exceptions of Personal Data/Sensitive Personal Data-

- Any information freely available in the public domain
- Any reviews, comments, messages, or blogs posted by customers on public sections of the Bank's website or application become published content and are not considered personal or sensitive data subject to this document.

3. What Personal Data does the Bank Collect & Process?

The Bank collects and processes the following categories of Personal Data of Data Principals for providing wholesale banking products and related services. Please note this list is indicative and not exhaustive and may be updated based on the nature of products, services, regulatory requirements, or applicable laws:

i. **Promoters/ partners/ proprietors/ directors** - name, father/ spouse name, date of birth, gender, marital status, address, mobile number, email ID, photograph, signature, PAN, Aadhaar, passport, voter ID, driving licence, or other KYC documents, category (SC/ST/OBC/Minority), religion, employment details, occupation, educational qualifications, income details such as annual income or salary slips or income tax returns or Form 16, land deed.

ii. **Guarantors** - name, father/spouse name, address, mobile number, gender, PAN, Aadhaar Number, account statement.

4. Where does the bank obtain Personal Data from?

Most of the personal data processed by the Bank is provided directly by you through our website, by visiting our branches, through our authorized third parties (such as DSAs and CSAs), through Relationship Managers, Marketing Officers or while availing and using our products and services. We may also collect certain information through cookies when you visit our website. In addition, we may collect information about you from other sources as described below, and after verifying its authenticity, may add it to the data we already hold and process it in accordance with this Privacy Policy.

Where personal data is obtained from third-party service providers for the purpose of offering relevant products, marketing content, offers, or services, such processing will be carried out only with your consent, wherever required. These third parties may include email service providers, credit information companies (such as CIBIL), financial institutions, subsidiaries, affiliates or associates of UBI, and authorized partners involved in activities such as co-lending, pool buyout, refinancing of loans and provisioning of government schemes.

5. Purpose for collecting and processing Personal Data

The Bank processes your Personal Data for the following purposes:

- Provide wholesale banking products and assist in and administer the provision of services to you, which includes activities like MSME loan provisioning, customer onboarding, and service facilitation:
  - To onboard the corporate customer and process wholesale services.
  - To assess eligibility, including income, creditworthiness, and other applicable criteria.
  - To capture, verify, and maintain guarantors' details where applicable.
  - To obtain and verify credit information from CIBIL or other credit information bureaus.
  - To conduct customer due diligence and risk profiling in line with regulatory requirements.
  - To create, issue, manage, and service the loan account.
  - To maintain records and reconcile accounts.
  - To provide and manage insurance or protection benefits linked to the loan.
  - To provide general banking services.

- Prevent, detect, investigate and prosecute fraud and alleged fraud, money laundering and other crimes and to verify your identity which includes KYC, compliance, and fraud related activities:
    - To verify and update customer contact details.
    - To conduct due diligence and investigations.
    - To fulfil legal obligations and provide data to auditors.
    - To facilitate Re-KYC and investigate staff accountability.
    - To monitor transactions and comply with regulatory reporting obligations.
    - To monitor and manage stressed loan accounts.
    - To identify early signs of financial distress.
- Providing information about products, offers, promotions, and services, which includes marketing and outreach activities in accordance with the consent provided by you.
- Process and deal with any complaints or enquiries made by or about you which includes grievance redressal and customer support:
    - To handle customer complaints and RCA.
    - To reach out to customers to recover the dues.
    - To recover the dues and manage the defaults.
    - To investigate and redress grievances.
- To analyse your Personal Data for Anti-Money Laundering (AML) and other regulatory compliance requirements, provisioning of services, assessing loan and credit eligibility, and for other legitimate business purposes necessary to support the Bank's operations.
- For reporting to regulatory authorities and internal audits.

6. Sharing of Personal Data

The Bank may disclose your Personal Data to various categories of third parties after obtaining your consent for the same or as part of legitimate use as per DPDPA. However, the Bank may also disclose your Personal Data without your consent where such disclosure is required under applicable laws, where the Bank is mandated to cooperate with statutory, regulatory, or governmental authorities, or where such disclosure is necessary for the legitimate use under the DPDP Act. The third parties include:

- **Other Group Companies, Partners, and Subsidiaries** for providing or enhancing products, services, and customer experience.
- **Sub-contractors, agents, or service providers** who work for the Bank or provide services/products on behalf of the Bank such as valuers, lawyers, CPVs, Chartered Accountants, Agencies for specialized monitoring, stock auditors, Techno Economic Valuers, etc.
- **Partners offering co-lending services, pool buyouts, or government backed programs**, where such sharing is necessary to deliver the offering.

- **Agents or service providers** engaged for activities connected to customer servicing, operational support, marketing (where permissible), or other contractual obligations.
- **Law enforcement agencies**, **government authorities**, **investigating agencies**, and any authority empowered under law.
- **Regulators**, including the **Reserve Bank of India**, Indian or overseas regulatory bodies, auditors, and entities appointed by regulators to conduct inspections, audits, or investigations.
- **Courts, tribunals, judicial or quasi-judicial bodies**, arbitrators, and arbitration tribunals.
- **Credit information companies / credit bureaus**, statutory bodies, and any persons or entities to whom disclosure is mandatory under applicable laws.
- Situations involving **regulatory reporting**, compliance with legal processes, or to **assert or defend the Bank's legal rights and interests**.

7. Withdrawal of Consent

Any individual has the right to withdraw their consent for the processing of their Personal Data at any time. Such withdrawal applies specifically to processing carried out for purposes, such as marketing or promotional communications, and will take effect only for future processing activities. It will not affect the lawfulness of any processing that was carried out prior to the withdrawal of consent. Even after consent is withdrawn, the Bank may continue to process Personal Data where required to comply with legal or regulatory obligations, to protect the Bank's lawful interests, to pursue available remedies, or to defend against existing or potential claims.
In accordance with the requirements of the Digital Personal Data Protection Act, 2023, a clear and accessible mechanism for withdrawal of consent is required. Data Principals may withdraw or modify their consent at any time by using the consent management option available on the corporate website, internet banking portal, mobile banking application, among others.

8. Processing of Personal Data of Children and Persons with Disability

We obtain verifiable consent from a parent or lawful guardian before processing the Personal Data of minors. We ensure that such processing does not have any detrimental effect on the child's well-being. The Bank does not engage in profiling, behavioural monitoring, or targeted advertising directed at children, and their data is not used for marketing or promotional activities. In line with the principle of data minimisation, only essential information required for providing the requested services is collected.

Where the individual is a Person with Disability who is unable to provide legally valid consent, we obtain verifiable consent from the lawful guardian before processing their Personal Data. Such processing is carried out with due care to ensure that it does not adversely impact the individual's well-being.

9. Use of Cookies

- We use cookies and similar technologies to enhance your browsing experience, analyse site traffic, and personalised content. Some cookies are essential for this site to function, while others help us understand your use and preferences enabling us to improve our services. These are stored locally on your computer or mobile devices. By clicking "Accept All", you consent to the storage of cookies on your device & its functionality. To customize your cookie preference, click "Customize" and select the categories you want to accept. You may choose to manage your preferences or modify/ withdraw your consent at any time by accessing cookie settings in your device.
- The Bank is not responsible for cookies placed in the device of user/s by any other website and Personal Data collected thereto. We do not control these cookies and once you have clicked on the advertisement and left the site, our Privacy Policy no longer applies.

10. Personal Data Security

- The Bank is committed to protecting your Personal Data in our custody. We take reasonable steps and procedural safeguards that meet applicable laws to ensure appropriate physical, technical and managerial safeguards are in place to protect your Personal Data confidentiality and integrity. Appropriate contracts inclusive of security measures to protect your Personal Data is executed with the third parties/ vendors/ service providers involved in providing services to us.
- The Bank has adopted ISO/IEC 27001 standards, which are globally accepted standards. The Bank's Datacentres, IT and Support functions are ISO 27001:2013 certified.

11. Data Principal Rights

We are committed to ensuring that you are aware of and can exercise your rights regarding your personal data.

Data principals have the following rights about their personal Data:

- **Right of Access**: Data principals have the right to obtain a copy of any or all the data bank processes about them, including the purpose for processing, the categories of personal data processed, any recipients of their data.
- **Right to Rectification**: Data principals have the right to request the correction of any inaccurate personal data held by bank.
- **Right to Erasure**: Data principals can request erasure of their personal data that is no longer required for legal, regulatory, or justified operational record-keeping purposes.
- **Right to Nominate**: Data principals have right to nominate a representative in case of death or incapacity.
- **Right to Grievance Redressal:** Before exercising the Right to Grievance, the Data Principal should first utilize the mechanisms available for other applicable rights.

When submitting a grievance request, the Data Principal must provide the ticket or reference number associated with the previous request.

To exercise any of the data principal rights, customer can visit corporate website, internet banking portal, mobile banking application, among others and can contact the Data Protection Officer (DPO) via:

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

If a satisfactory response is not received within 90 days under the grievance redressal system as per Rule 14 of DPDP Rules, you may lodge a complaint before the Data Protection Board for the redressal of any grievance arising from a personal data breach, the exercise of your statutory rights, or the failure to comply with applicable obligations.

12. Retention of Personal Data

The Bank may retain your Personal Data for as long as required for legitimate purposes that may include such as managing your account and dealing with any concerns that may arise or otherwise if as may be required for any for legal, regulatory and/or statutory reasons.

If the Bank no longer requires the retention of the information provided by the Customer, it will use best efforts to destroy or delete such Customer Information as per our Bank's internal policies.

13. Links to other Websites and Social Media

The Bank website may contain links to websites of other organizations that are not owned by Bank. This document does not cover how those organizations process your Personal Data. We encourage you to read the relevant privacy notice on the other websites that you may visit.

Please note that when visiting Bank's official social media site/ page, you are subject to this document well as the social media platform's own terms and conditions.

14. Conflict of Laws & Disputes

You agree that, irrespective of your location or country of jurisdiction, this document and its contents shall be subject to and governed by Indian laws (as amended from time to time) as may be applicable and that you waive all your rights which you may have in relation to this document under any contract or relevant laws applicable to the jurisdiction where you are situated and/or by which you are governed.

Any disputes over inter alia collection, storage and handling of Personal Data will be governed by this document, Terms and Conditions and by the laws of India and courts of India shall have exclusive jurisdiction.

15. Grievance Redressal

In case of any discrepancies or grievances, you may contact us at

- Email: dpoffice@unionbankofindia.bank.in
- Address: Union Bank of India building, 2nd Floor, Data Protection Office, Military Road, Marol, Andheri East, Mumbai – 400059

16. Notification of Changes

We may update this Privacy Policy from time to time to reflect changes in our business, technology, or legal requirements. We encourage you to review this Privacy Policy regularly to stay informed about our privacy practices and any changes we may make.

This Privacy Notice was last updated on July 31, 2026.