External Privacy Notice

United Bank Limited – Qatar

Effective Date: 2026 | Version 1.0

Who we are

United Bank Limited, Qatar ("UBL Qatar", "Bank", "we", "us" or "our") is committed to protecting the privacy and personal data of its customers, prospective customers, authorised representatives and other individuals ("Customer" or "you") in accordance with Law No. (13) of 2016 on Protecting Personal Data Privacy ("PDPPL"), its implementing guidelines issued by the Ministry of Communications and Information Technology ("MCIT"), and the Consumer Protection instructions issued by the Qatar Central Bank ("QCB") pursuant to the Law of Qatar Central Bank and the Regulation of Financial Institutions promulgated by Law No. (13) of 2012 ("QCB Law"), Qatar Central Bank Data Handling and Protection Regulation (2025) and applicable circulars.

All bank employees, affiliates, and service providers are legally obligated to treat customer data with the highest standard of confidentiality. As such, customer data will only be accessed by authorized personnel on a need-to-know basis, and your onboarding records and documents fall under our highest confidentiality classification.

What data we collect

Identity and contact details, financial and transaction data, KYC and due diligence information, employment and business data, device and digital data, biometric data (for identity verification), and communications records.

Why we collect it

To open and operate your account and provide banking services; to comply with QCB AML/CFT law, regulations and tax reporting obligations; to detect and prevent fraud; and , where you have consented, to send you marketing communications.

Who we share it with

UBL group companies, regulatory and law enforcement authorities, third-party service providers (payment processors, technology providers, KYC services), correspondent banks, credit reference agencies and insurance providers. We never sell your data.

How long we keep it

A minimum of 10 years from the end of your relationship with us, in line with QCB AML/CFT and other regulatory requirements.

Your rights

You have the right to access, correct, delete, restrict, or port your data, to object to certain processing, including automated processing, and to withdraw consent at any time. To exercise any right, email dpo_qatar@ublint.com . We will respond within 30 days.

This Privacy Notice explains what personal data we collect, how we use it, with whom we share it, and the rights available to you. By opening or maintaining an account with us, or by using any of our products, services, platforms or digital channels, you acknowledge that you have read and understood this Privacy Notice.

1. Data Controller

The data controller responsible for your personal data is United Bank Limited – Qatar, a foreign bank branch licensed and regulated by the Qatar Central Bank ("QCB"). Our registered contact details for data privacy matters are set out in Section 17 of this Notice.

2. Definitions

The following words and phrases shall have the meanings stated below and are as defined within the PDPPL, when used in this Privacy Notice:

"Personal Data" - means any information relating to an identified or identifiable natural person, including but not limited to name, identification number, location data, online identifiers, financial data, or factors specific to the physical, economic, cultural or social identity of that person, as defined under the PDPPL.

"Processing" - means any operation or set of operations performed on Personal Data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure, restriction, erasure or destruction.

"Sensitive Personal Data" - means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health data, biometric data, genetic data, data concerning a person's sex life or sexual orientation, or criminal record data, as defined under the PDPPL.

"QCB" - means the Qatar Central Bank, established pursuant to Law No. (13) of 2012 on Qatar Central Bank and the Regulation of Financial Institutions.

"PDPPL" - means Law No. (13) of 2016 on Protecting Personal Data Privacy, together with the implementing guidelines issued by the Ministry of Communications and Information Technology, as amended from time to time.

"NCGAA" - means the National Cyber Governance and Assurance Affairs, a division of the National Cyber Security Agency (NCSA), which performs the duties of the Competent Authority for the purposes of supervising the processing of personal data within the State of Qatar under the PDPPL.

"Services" - means all banking products, services, digital channels, platforms, applications and facilities offered by UBL Qatar to Customers from time to time.

3. Personal Data We Collect

We collect and process the following categories of Personal Data, subject to applicable legal requirements:

a) **Identity and Contact Data:** full legal name; date of birth; nationality; passport number, Qatar National ID card (QID) number or other national identification number; residential address; telephone number; email address; and specimen signature.

b) **Financial and Transaction Data:** bank account details; credit and debit card information; account balances; transaction history; income details; source of funds and source of wealth declarations; credit history; and investment profile.

c) **Know Your Customer (KYC) and Due Diligence Data:** copies of identification documents; proof of address; tax identification numbers; politically exposed person (PEP) status; sanctions screening results; and customer risk classification.

d) **Employment and Business Data:** employer name and address; occupation; business registration details; beneficial ownership information; and professional licence numbers where applicable.

e) **Device and Digital Data:** IP address; device identifiers; browser type; operating system; access logs; cookies and similar tracking technologies; location data (where enabled); and usage data from our digital channels and mobile application.

f) **Biometric Data:** fingerprint data or other biometric identifiers collected in accordance with applicable Qatar law for identity verification purposes at our branches or through authorised third-party verification services.

g) **Communications Data:** records of telephone calls (which may be recorded), correspondence, complaints, and enquiries made to or by you in connection with our Services.

h) **Sensitive Personal Data:** we process Sensitive Personal Data only where strictly necessary, for example health information in connection with insurance or accessibility requirements, or criminal record data as required by our AML/CFT obligations. We will seek your explicit consent where required by law.

Where certain data is not disclosed, this may result in the Banks inability to open or maintain your account due to AML/KYC obligations.

4. How We Collect Personal Data

We collect Personal Data from the following sources:

a) **Directly from you:** when you complete an Account Opening Form, application form or other Bank documentation; when you use our branches, ATMs, digital channels, mobile application or

telephone banking; when you correspond with us by any means; and when you respond to surveys or promotions.

b) **Automatically:** through our digital channels, website, mobile application and ATMs using cookies, web beacons, logs and similar technologies, as further described in Section 13 of this Notice.

c) **Third parties and public sources:** credit reference agencies; government identity databases; sanctions and PEP screening providers; fraud prevention agencies; employers; introducers; correspondent banks; and other financial institutions, where permitted by law.

d) **Regulatory and Law Enforcement Bodies:** where we are required or permitted by applicable law to obtain information from the QCB, the Qatar Financial Information Unit ("QFIU"), or other governmental or regulatory authorities of the State of Qatar.

5. Legal Basis for Processing

We process your Personal Data on the following legal bases under the PDPPL and applicable law:

a) **Contractual Necessity:** processing is necessary for the performance of a contract to which you are a party, or in order to take steps at your request before entering into a contract with us. This includes opening and operating your account, processing transactions, issuing cards and providing all contracted banking services.

b) **Legal Obligation:** processing is necessary for compliance with a legal obligation to which we are subject, including obligations under Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and its implementing regulations (collectively, "AML/CFT Law"), QCB regulations, tax reporting obligations (including FATCA and CRS), and court orders.

c) **Legitimate Interests:** processing is necessary for the purposes of our legitimate interests or those of a third party, provided such interests are not overridden by your interests or fundamental rights. This includes fraud detection and prevention, security monitoring, network and information security, credit risk management, and improving our services and digital channels.

d) **Consent:** where we rely on your consent as the legal basis, we will seek your explicit and informed consent prior to processing. You may withdraw your consent at any time without affecting the lawfulness of processing prior to withdrawal. Withdrawal of consent may affect your ability to access certain optional services.

e) **Vital Interests:** in exceptional circumstances, we may process Personal Data where necessary to protect your vital interests or those of another person.

f) **Public Interest:** processing may be necessary for the performance of a task carried out in the public interest or in the exercise of official authority, including regulatory reporting and supervisory activities.

e) **Parental, Guardian and Joint Account Consent:** Where a Customer is a minor (under 1 years of age) or is otherwise legal required to act through an authorized representative, the consent of a parent, legal guardian or court-appointed representative will be obtained in place of, or in addition to, the Customer's own consent, in accordance with applicable Qatar law.

Where an account is held jointly or is linked to a dependent relationship, each account holder or authorized representative will be provided with this Privacy Notice and will be required to consent to the processing of their personal data separately. Joint account holders acknowledge that certain personal data relating to the account, including transaction history and account balances, will be accessible to and processed in respect of all parties to the account.

Processing of a minor's personal data will be limited to what is strictly necessary for the provision of the relevant banking product or service. Where a minor reaches the age of 18, we will seek fresh consent directly from the individual in accordance with section 5d of this Notice.

6. How We Use Your Personal Data

We use your Personal Data for the following purposes:

a) **Account and Service Management:** to open, operate, maintain and close your account(s); to process transactions, payments and transfers; to issue and manage cards; to provide internet banking, mobile banking and telephone banking services, to periodically review/update customer information and KYC records during the relationship lifecycle; and to administer all products and services you hold with us.

b) **Identity verification and KYC compliance:** to verify your identity in accordance with the Qatar AML/CFT Law, QCB regulations and the Bank's internal policies; to conduct ongoing due diligence; and to screen against applicable sanctions lists and PEP databases.

c) **Credit Assessment and Risk Management:** to assess creditworthiness; to manage credit risk; to conduct credit reference checks; and to make decisions regarding the provision of lending or other credit facilities.

d) **Regulatory Compliance and Reporting:** to meet our obligations under Qatar law and applicable international standards, including tax reporting under FATCA (to the US Internal Revenue Service) and the Common Reporting Standard (CRS); to report suspicious transactions to the Qatar Financial Information Unit (QFIU); and to comply with QCB supervisory requirements.

e) **Fraud Prevention and Security:** to detect, investigate and prevent fraudulent transactions, financial crime, unauthorised access and other illegal activities; to manage and operate security systems including physical and digital security; and to protect the interests of the Bank and its customers.

f) **Customer Communications:** to communicate with you regarding your account, transactions, service updates, regulatory disclosures, and responses to your enquiries and complaints.

g) **Marketing and Product Development**: where you have provided consent or where we have a legitimate interest, to inform you of products, services and promotions offered by UBL Qatar or its group companies that may be of interest to you; and to conduct market research and customer satisfaction surveys.

h) **Analytics and Service Improvement:** to analyse usage patterns of our digital channels; to improve our products, services and customer experience; and to conduct internal reporting and business planning.

i) **Legal Proceedings and Dispute Resolution:** to establish, exercise or defend legal claims; to respond to regulatory investigations; and to comply with court orders or binding determinations of regulatory bodies.

7. Sharing Your Personal Data

We may share your Personal Data with the following categories of recipients, strictly on a need-to-know basis and subject to appropriate safeguards:

- **UBL Group Companies:** we may share data with other entities within the United Bank Limited group of companies for the purposes of providing integrated banking services, risk management, compliance and internal reporting.
- **Regulatory and Governmental Authorities:** we are required by law to share information with the QCB, the Qatar Financial Information Unit (QFIU), the National Anti-Money Laundering and Terrorism Financing Committee (NAMLC), tax authorities (including for FATCA and CRS purposes), courts, and law enforcement agencies of the State of Qatar.
- **Third-Party Service Providers:** we engage reputable third-party providers to assist in delivering our services, including payment processors, card scheme operators (including Visa), technology and IT service providers, cloud service providers, identity verification and KYC service providers, credit reference agencies, fraud prevention services, audit and advisory firms, and legal counsel. These parties are contractually bound to process your data only for specified purposes and in accordance with applicable law.
- **Correspondent and Partner Banks**: where transactions require correspondent banking relationships, relevant transaction data will be shared with correspondent banks as necessary to process the transaction.

- **Insurance Providers:** in connection with any insurance product linked to your account, we may share relevant data with the nominated insurance provider, subject to the terms of the Customer Insurance Communication.
- **Credit Reference Agencies:** we may share information with licensed credit reference bureaux operating in Qatar to conduct credit checks and to report account conduct as required or permitted by QCB regulations.
- **Other Financial Institutions:** where required to investigate or resolve disputes, prevent fraud, or comply with legal obligations, we may share information with other banks or financial institutions.

We do not sell your Personal Data to third parties for commercial purposes. Any disclosure will be made strictly in accordance with applicable law and this Privacy Notice.

8. International Transfers of Personal Data

a) In providing banking services, it may be necessary to transfer your Personal Data to recipients located outside the State of Qatar, including to correspondent banks, group companies, card schemes, through cloud providors or service providers in other jurisdictions.

b) Transfers of Personal Data outside the State of Qatar are subject to the requirements of the PDPPL. Where we transfer Personal Data outside Qatar, we will ensure that adequate safeguards are in place in accordance with the PDPPL.

These safeguards may include:

- transfers to countries or territories that provide an adequate level of data protection as assessed by the QCB under the PDPPL;
- contractual clauses approved or recognised under the PDPPL; binding corporate rules within the UBL group;
- or the prior permission of the QCB;

These safeguards are required for the performance of your banking contract (for example, to process international payments through SWIFT or correspondent banking networks).

You may request further information regarding international transfer safeguards by contacting us as set out in Section 17.

9. Retention of Personal Data

a) We retain your Personal Data for as long as is necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying legal, regulatory, accounting or reporting requirements.

b) In accordance with the QCB's instructions and the Qatar AML/CFT Law, we are required to retain Customer identification records and transaction records for a minimum of ten (10) years from the date on which the business relationship ends or from the date of the occasional transaction, or such longer period as may be required by applicable law or a regulatory direction.

c) Account statements, correspondence and transaction records will generally be retained for a period of not less than ten (10) years following closure of the account, unless a longer period is required by law, regulation or ongoing legal proceedings.

d) Where Personal Data is processed on the basis of consent, it will be retained until consent is withdrawn, unless there is another legal basis for continued retention.

e) Upon expiry of the applicable retention period, Personal Data will be securely deleted, destroyed or anonymised in accordance with our data retention policy, except where retention is required to comply with a legal obligation, court order or regulatory direction.

10. Your Rights Under the PDPPL

Subject to applicable law and the conditions prescribed under the PDPPL, you have the following rights in relation to your Personal Data:

- **Right of Access:** you have the right to request confirmation of whether we process your Personal Data and, if so, to obtain a copy of that data together with information about how it is processed.
- **Right to Rectification**: you have the right to request that inaccurate or incomplete Personal Data held by us be corrected or completed without undue delay.
- **Right to erasure:** you have the right to request the deletion or destruction of your Personal Data in certain circumstances, for example where the data is no longer necessary for the purpose for which it was collected, or where you withdraw consent and there is no other legal basis for processing. This right is subject to our legal and regulatory retention obligations.
- **Right to restriction of processing:** you have the right to request that we restrict the processing of your Personal Data in certain circumstances, for example where you contest the accuracy of the data or where processing is unlawful but you do not wish the data to be deleted.
- **Right to data portability:** you have the right to receive your Personal Data in a structured, commonly used and machine-readable format, and to transmit that data to another controller, where the processing is based on consent or contract and is carried out by automated means.
- **Right to object:** you have the right to object to processing of your Personal Data where it is based on legitimate interests, or to processing for direct marketing purposes.
- **Right to withdraw consent**: where processing is based on your consent, you have the right to withdraw consent at any time, without affecting the lawfulness of processing prior to withdrawal.
- **Rights in relation to automated decision-making**: you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects you, except where such processing is necessary for entering into or performing a contract, authorised by law, or based on your explicit consent. Further details are set out in Section 11 below.

To exercise any of the above rights, please submit a written request to us as set out in Section 17. We will respond to your request within the timeframes prescribed under the PDPPL, generally within thirty (30) days of receipt of a valid request. We may need to verify your identity before processing your request. In certain circumstances, we may be entitled to refuse your request; if so, we will explain the reason in writing.

11. Automated Decision-Making and Profiling

a) We may use automated processing and profiling in connection with credit assessment, fraud detection, sanctions screening and the assessment of money laundering or terrorist financing risk. In such cases, automated processing may result in a decision that affects your access to, or the terms of, our products and services.

12. Security of Your Personal Data

a) We implement appropriate technical and organisational measures to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These measures include encryption of data in transit and at rest, access controls, multi-factor authentication for digital channels, physical security at our premises, staff training, and regular security assessments.

b) All third-party service providers who process Personal Data on our behalf are contractually required to implement equivalent security measures and to process data only on our instructions.

c) In the event of a Personal Data breach that is likely to result in a risk to your rights and freedoms, we will notify you and the NCGAA as required under the PDPPL, within the prescribed timeframe of 72 hours.

Where an incident occurs in relation to your data, we will also notify the QCB in accordance with applicable QCB cybersecurity instructions. This includes reporting the incident within 1 hour

where the risk is high, within 4 hours where the risk is medium, and reporting all low risk incidents on a monthly basis.

d) You are responsible for maintaining the confidentiality of your banking credentials, PINs, passwords and one-time passcodes. You should not disclose these to any person and should notify us immediately if you believe your credentials have been compromised.

13. Cookies and Online Tracking

a) Our website and digital channels use cookies and similar tracking technologies. Cookies are small text files placed on your device that help us recognise returning visitors, remember your preferences, and understand how our digital channels are used.

b) We use the following categories of cookies: (i) Strictly Necessary Cookies, which are essential for our digital channels to function and cannot be disabled; (ii) Functional Cookies, which remember your preferences and settings; (iii) Analytics Cookies, which help us understand usage patterns to improve our services; and (iv) Third-Party Cookies, which are set by third-party services integrated into our website, including LinkedIn, Meta (Facebook), and YouTube.

c) Non-essential cookies will only be placed on your device with your consent, obtained through our cookie consent banner. You may withdraw or amend your cookie preferences at any time by accessing your cookie settings. Note that disabling certain cookies may affect the functionality of our digital services.

d) For full details of the cookies we use, including cookie names, durations, purposes and third-party providers, please refer to our Cookie Policy available on the UBL website.

14. Marketing Communications

a) We may send you information about our products, services and promotions where you have provided your consent, or where we have a legitimate interest in marketing similar products and services to existing customers, subject to your right to object.

b) You may opt out of receiving marketing communications at any time by: notifying us in writing at the contact details in Section 17; visiting your nearest UBL Qatar branch; calling our Phone Banking service; or using the unsubscribe facility in any marketing email.

c) Opting out of marketing communications will not affect the delivery of service-related communications required in connection with your account, including transaction alerts, account statements, regulatory disclosures and fraud notifications.

15. Consumer Protection and Regulatory Oversight

UBL Qatar is subject to the consumer protection instructions issued by the QCB pursuant to the QCB Law and all related circulars and guidance. We are committed to treating our customers fairly, transparently and with respect in all our data processing activities.

In accordance with QCB Consumer Protection instructions, we will:

i. provide you with clear and accessible information about how your Personal Data is used;

ii. not use your Personal Data in a manner that is misleading, unfair or contrary to your interests;

iii. process your Personal Data only for legitimate purposes disclosed to you;

iv. implement appropriate safeguards to protect your Personal Data; and

v. respond to your data-related enquiries and complaints in a timely and transparent manner.

If you have a complaint regarding the handling of your Personal Data, you may:

i. submit a complaint to us using the contact details in Section 17, and we will acknowledge your complaint within three (3) business days and aim to resolve it within fifteen (15) business days;

ii. if your complaint is not resolved to your satisfaction, you may escalate your complaint to the QCB Banking Customer Services Protection Department by telephone on +974 4445 6412 or via the QCB's website at www.qcb.gov.qa; or

iii. exercise your rights under the PDPPL by submitting a complaint to the National Cyber Governance and Assurance Affairs (NCGAA) of the National Cyber Security Agency (NCSA) via www.ncsa.gov.qa.

16. Changes to This Privacy Notice

a) We may update this Privacy Notice from time to time to reflect changes in our data processing practices, applicable law, regulatory requirements or the services we offer. The "Effective Date" at the top of this Notice indicates when the most recent revision was made.

b) We will provide notice of material changes to this Privacy Notice by: displaying a prominent notice on our website and digital channels; providing notice via SMS Alert or email to the contact details registered with us; or by such other means as required by applicable law.

c) In accordance with Clause 34 of the Terms and Conditions Governing Bank Account, a sixty (60) day notice period will apply to any revision, amendment or supplement to this Notice, following issuance of the Bank Notice to your registered

address, email or SMS number. Your continued use of our banking services after the end of the Notice Period shall constitute your acceptance of the revised Privacy Notice.

d) We encourage you to review this Privacy Notice periodically. The most current version will always be available on the UBL Qatar website and at our branches upon request.

17. Contact Us and Data Privacy Enquiries

For any enquiries, requests or complaints regarding this Privacy Notice or the processing of your Personal Data, please contact us using the following details:

United Bank Limited – Qatar

Data PrivacyOfficer

Website: www.ubldigital.com/qatar-home

Email: dpo_qatar@ublint.com

Phone Banking: As communicated via the UBL Qatar website and branches

For complaints to the QCB Banking Customer Services Protection Department:

Website: www.qcb.gov.qa

Emai: cp@qcb.gov.qa,

Telephone: +974 4445 6412 / +974 4445 6456

18. Governing Law and Jurisdiction

This Privacy Notice is governed by the laws of the State of Qatar, including the PDPPL, applicable QCB regulations, and other relevant laws and regulations of the State of Qatar.

Any dispute or difference between the parties arising out of or in connection with this Privacy Notice shall be subject to the non-exclusive jurisdiction of the courts of the State of Qatar, without prejudice to any regulatory or supervisory jurisdiction of the QCB, the NCGAA or other competent authority.

© 2026 United Bank Limited – Qatar. All Rights Reserved.