Data Privacy Policy
For
Sharaf Exchange Mobile Application

1. Our Commitment to Your Privacy

Sharaf Exchange LLC (hereinafter called "**Sharaf Exchange**" or "**We**" or "**Our**") prioritizes your privacy. This Privacy Policy explains the data we collect, its usage, and your rights regarding your Personal Data. We are dedicated to maintaining the confidentiality, integrity, and security of the Personal Data you provide. Sharaf Exchange is committed to handling your data securely and this policy is aligned with the UAE Federal Decree Law No. 45 of 2021 on Personal Data Protection (PDPL), and Central Bank of UAE (CBUAE) regulations, including the Consumer Protection Regulations (and associated standards, Circular No. 8 of 2020).

In the context of this Privacy Policy and these Terms and Conditions, "**you**" or "**your**" refers to the individual who is using the services of Sharaf Exchange, including but not limited to accessing the mobile application relating to our exchange facilities, including remittance, ("Mobile App"), conducting transactions, or interacting with Sharaf Exchange through any of its platforms or service channels. It includes any customer whose personal data is collected, processed, or stored by Sharaf Exchange.

2. Definitions

This Definitions section applies to and governs all capitalized terms used in this Privacy Policy and any related terms, schedules, notices, and communications for the Mobile App. To the extent of any inconsistency with earlier definitions in this Privacy Policy, this section shall prevail.

2.1 "Adequacy Decision" means a decision by a competent authority recognizing that a foreign jurisdiction offers an adequate level of protection for Personal Data under applicable law.

2.2 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with Sharaf Exchange.

2.3 "AML/CFT" means Anti-Money Laundering and Combating the Financing of Terrorism obligations under applicable law (including UAE Decree Federal Law No. 20 of 2018 and Cabinet Decision No. 10 of 2019, as amended).

2.4 "Analytics" means tools and techniques used to measure usage, performance, and improve services for the Website/App.

2.5 "App" or "Mobile App" means the mobile application(s) provided by or on behalf of Sharaf Exchange which is the subject matter of this Data Privacy Policy.

2.6 "Applicable Law" means all laws, regulations, regulatory guidance and standards applicable to the Mobile App, including the PDPL and CBUAE Consumer Protection Regulations and Standards.

2.7 "Automated Decision-Making" means a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects concerning an individual.

2.8 “CBUAE” means the Central Bank of the United Arab Emirates.

2.9 “Complaint” means a written or recorded expression of dissatisfaction regarding Personal Data processing or customer service that requests a response or resolution.

2.10 “Consent” means any freely given, specific, informed, and unambiguous indication of the Data Subject’s wishes, signifying agreement to the processing of Personal Data for a stated purpose, which can be withdrawn at any time.

2.11 “Controller” or “Data Controller” means the person or entity that determines the purposes and means of Processing Personal Data (Sharaf Exchange acts as Controller for the Mobile App as described in this Policy).

2.12 “Cookies” means small text files stored on a device to support functionality, security, and preferences, and—where consented—analytics and marketing.

2.13 “Customer”, “Consumer”, “You” or “Your” means the individual using the services of Sharaf Exchange in relation to the Mobile App, whose Personal Data is collected, processed, or stored.

2.14 “Data Breach” or “Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

2.15 “Data Office” means the UAE Data Office established under the PDPL.

2.16 “Data Protection Officer” or “DPO” means the person appointed by Sharaf Exchange, where required, to oversee compliance with applicable data protection laws and to serve as a contact point with the Data Office.

2.17 “Data Subject” means an identified or identifiable natural person to whom the Personal Data relates.

2.18 “Data Subject Request” or “DSR” means a request from a Data Subject to exercise rights under applicable law (e.g., access, rectification, erasure, restriction, objection, portability, or withdrawal of Consent).

2.19 “De-identification” or “Pseudonymization” means processing Personal Data so it can no longer be attributed to a specific Data Subject without the use of additional information kept separately and subject to technical and organizational measures.

2.20 “Deletion” means permanent removal of Personal Data so that it cannot be reconstructed or retrieved in the ordinary course.

2.21 “Do Not Contact List” means an internal suppression list maintained by Sharaf Exchange to record opt-outs from marketing communications.

2.22 “Encryption” means applying cryptographic techniques to render data unreadable to unauthorized parties in transit and/or at rest.

2.23 “FIU” means the UAE Financial Intelligence Unit.

2.24 “International Data Transfer” means the transfer of Personal Data to a country or territory outside the UAE.

2.25 “Legitimate Interests” means interests pursued by Sharaf Exchange or a third party that are balanced against the rights and freedoms of the Data Subject, consistent with PDPL.

2.26 “Minors” means individuals under the age specified by applicable UAE law for valid consent, unless parental or guardian authorization applies.

2.27 “Mobile App” has the meaning given to App.

2.28 “OFAC” means the United States Office of Foreign Assets Control.

2.29 “Partner” means any third parties that support issuance, processing, or servicing of the Mobile App.

2.30 “PDPL” means UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, together with related regulations and guidance.

2.31 “Personal Data” means any data relating to an identified or identifiable natural person.

2.32 “Privacy Policy”, or “Policy”, means this Data Privacy Policy.

2.33 “Processing” means any operation performed on Personal Data, whether by automated means or not, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

2.34 “Processor” or “Data Processor” means a person or entity that processes Personal Data on behalf of the Controller according to documented instructions.

2.35 “Profiling” means automated processing of Personal Data to evaluate certain aspects relating to an individual, in particular to analyze or predict performance, economic situation, health, preferences, interests, reliability, behavior, location, or movements.

2.36 “Sanctions Lists” means lists maintained by competent authorities, including the United Nations, UAE Local List, EU, OFAC, and other applicable sanctions authorities.

2.37 “Security Incident” means an event that compromises the confidentiality, integrity, or availability of systems or data, including but not limited to a Personal Data Breach.

2.38 “Sensitive Personal Data” means categories of Personal Data designated as sensitive under PDPL and applicable law (for example, data revealing health, biometric identifiers, or other categories defined by law).

2.39 “Service Providers” means any third parties engaged by Sharaf Exchange to provide services to or for the Mobile App, subject to binding data protection obligations.

2.40 “Sharaf Exchange”, “We”, “Us”, or “Our” means Sharaf Exchange LLC, the Data Controller for the Mobile App as described in this Policy.

2.41 “Standard Contractual Clauses” means contractual provisions approved by a competent authority for International Data Transfers to ensure adequate safeguards.

2.42 “Terms and Conditions” means the applicable terms governing the Mobile App, as updated from time to time.

2.43 "Third Party" means any external entity or individual authorized to process data on behalf of Sharaf Exchange or otherwise involved in the Mobile App as described in this Policy.

2.44 "Tokenization" means substituting sensitive data elements with non-sensitive equivalents (tokens) that have no exploitable meaning or value.

2.45 "Transactional Data" means data related to financial transactions performed on the Mobile App, including merchant, ATM, load/reload, amounts, currency, and related metadata.

2.46 "UAE Local List" means the UAE list of designated persons and entities issued by competent authorities.

2.47 "Website" means www.sharafexchange.ae and any related pages that present information about or facilitate the Mobile App.

3. Information We Collect

We may collect the following types of personal and transactional data:

3.1 Identification and Contact Information: name, date of birth, nationality, Emirates ID/passport details, residential address, email address, and mobile phone number.

3.2 Verification and Compliance Information: Know Your Customer (KYC) documents; results of identity verification; sanctions-list and adverse media screening results; Politically Exposed Person (PEP) status (where applicable); and other Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) checks required by Applicable Law.

3.3 Financial and Credit Information: information received from government-authorized Transactional Information, Credit Information Agencies and related credit assessments, to the extent permitted by Applicable Law.

3.4 Device, Technical, and Usage Information: IP address; device identifiers; device type; operating system; app version; browser information; cookie identifiers; diagnostic logs; crash reports; and interactions with our Website/Mobile.

3.5 Communications and Customer Support Records: information contained in application forms; correspondence; emails; in-app messages/chats; recorded or monitored telephone calls (where permitted by law); internet communications; complaints; and service interactions.

3.6 Preferences and Marketing Information: your communication preferences and consents; opt-outs (including our Do Not Contact List status); survey responses; and campaign interaction data.

3.7 Analytics and Cookies Data: cookie preferences; analytics identifiers; and aggregated usage metrics collected via cookies/SDKs, as configured by your choices and consent.

3.8 Sensitive Personal Data (only where required by law or with your explicit consent): biometric identifiers used for identity verification (if applicable) and other categories designated as sensitive under PDPL. We do not intentionally collect health data for the Mobile App.

3.9 Inferences and Risk Profiles: inferences generated by us or our Partners for AML/CFT, fraud detection, credit/collections, service improvement, and program analytics (for example, risk scores and profiling indicators), subject to human review where legally required.

3.10 Legal and Compliance Records: records of sanctions screening, regulatory disclosures and requests, disputes, and responses to competent authorities.

3.11 Additional Information: other information necessary to provide services, operate the Mobile App, or comply with Applicable Law. If you choose not to provide required information, we may be unable to offer or continue the related services on the Mobile App.

4. How We Process Your Information

Your information is used for the following purposes:

4.1 Issue, activate, service, and manage your Mobile App and related accounts.

4.2 Conduct identity verification and ongoing due diligence, comply with anti-money laundering and countering the financing of terrorism (AML/CFT) and sanctions requirements.

4.3 Process exchange transactions, foreign exchange, loads/reloads, refunds, chargebacks, and dispute resolution activities.

4.4 Communicate mandatory notices and service messages (e.g., account updates, security alerts, service changes) and respond to your customer support requests.

4.5 Monitor, detect, investigate, and prevent fraud, financial crime, and security incidents; apply risk-based controls and transaction monitoring.

4.6 Operate, maintain, and improve our Website/Mobile, infrastructure, and user experience; perform diagnostics, quality assurance, and service analytics (in line with your cookie/analytics choices).

4.7 Provide or facilitate program features and benefits with our bank and scheme partners (for example, loyalty or points programs where applicable).

4.8 Conduct profiling and use automated tools (including real-time screening) to assess customer and transaction risk to support AML/CFT, fraud prevention, and regulatory obligations; any flagged cases are subject to human review where required by law.

4.9 Screen transactions, customers, and counterparties against applicable sanctions lists (including those issued by the United Nations, the UAE Local List, and OFAC), and comply with relevant Financial Action Task Force (FATF) recommendations and the Applicable Law.

4.10 Manage our relationship with you, enforce our Terms and Conditions, collect debts, and protect our rights, interests, and the security and integrity of our services.

4.11 Carry out planning, reporting, product development, service improvement, testing, training, and governance (using de-identified or aggregated data where feasible).

4.12 Comply with record-keeping, auditing, regulatory reporting, and responses to competent authorities, courts, and government-authorized Credit Information Agencies as required by law.

4.13 Send marketing and promotional communications with your consent (where required) and honor your preferences and opt-outs (see "Marketing and Communication Preferences").

4.14 Facilitate international data transfers using lawful transfer mechanisms and safeguards where processing outside the UAE is necessary to operate the Mobile App.

4.15 Maintain data accuracy and keep your contact details up to date; we may request updated information to meet legal or servicing requirements.

4.16 Processing of personal data is conducted under one or more lawful bases under UAE law, including:

(i) Performance of a contract (for example, Mobile App activation, servicing, and transactions).

(ii) Compliance with legal obligations (for example, AML/CFT, sanctions screening, record-keeping, and regulatory reporting).

(iii) Legitimate interests (for example, fraud prevention, security, risk management, analytics for service improvement, product development, business planning, and protecting our rights), balanced against your rights and freedoms.

(iv) Your consent (for example, direct marketing, non-essential cookies/analytics, and where required by law for certain international transfers). You may withdraw consent at any time.

4.17 Protection of vital interests or public interest where applicable under UAE law.

5. Sharing of Personal Data

We may share your Personal Data with Third Parties strictly on a need-to-know basis and only for lawful, specified purposes related to the Mobile App. Such sharing is subject to contractual, technical, and organizational safeguards as outlined below.

5.1 Service Providers and Processors: with vetted Service Providers acting as Processors (e.g., IT hosting, customer support, KYC/identity verification, analytics). These Third Parties are bound by written data protection agreements requiring: (a) processing only on Our documented instructions; (b) confidentiality obligations; (c) appropriate security measures; (d) restrictions on sub-processing without equivalent safeguards; (e) timely breach notification; (f) assistance with Data Subject Requests and regulatory compliance; and (g) secure return or Deletion of data at the end of services.

5.2 Payment Ecosystem Participants: with issuing/settlement banks, payment networks, correspondent institutions, merchants, acquirers, and dispute-resolution bodies to authorize, settle, refund, and investigate Transactions, chargebacks, and disputes, and to perform fraud prevention and risk controls.

5.3 Professional Advisors and Insurers: with auditors, legal counsel, consultants, and insurers for audit, assurance, claims handling, legal advice, risk management, governance, and corporate compliance.

5.4 Marketing Partners: where permitted by Applicable Law and based on valid Consent (where required) and subject to your preferences. We maintain a Do Not Contact List and honor your opt-out choices. We do not share Sensitive Personal Data for marketing without explicit Consent.

5.5 Aggregated/De-identified Data: with Third Parties for analytics, product development, and service improvement where data has been De-identified or aggregated so it no longer identifies you.

5.6 Sanctions/AML Compliance: with relevant authorities and counterparties for screening against applicable Sanctions Lists (including United Nations, UAE Local List, and OFAC), AML/CFT monitoring, and, where required, reporting to the FIU.

5.7 International Data Transfers: where Personal Data is transferred outside the UAE, we apply lawful transfer mechanisms consistent with PDPL (e.g., Adequacy Decisions, Standard Contractual Clauses, or other approved safeguards) and implement appropriate technical and organizational measures. Where explicit Consent is required by law for a specific transfer, we will obtain it in advance.

5.8 Minimum Necessary and Purpose Limitation: we disclose only the minimum Personal Data necessary to fulfill the stated purpose.

5.9 Onward Transfers: onward disclosures by recipients are prohibited unless permitted by law and subject to equivalent safeguards.

5.10 Independent Privacy Notices: each Third Party's use of your Personal Data may also be subject to its own privacy policy. We will provide or direct you to further information upon request.

5.11 Records of Disclosures: we maintain records of material disclosures as required by Applicable Law.

5.12 No Sale of Personal Data: we do not sell your Personal Data.

5.13 Sensitive Personal Data: we share Sensitive Personal Data only where required by law or with your explicit Consent.

5.14 Your Choices: you may request information about categories of recipients to whom your Personal Data has been disclosed, subject to Applicable Law (see "Data Subject Requests").

6. International Data Transfers

6.1 You acknowledge and agree that only residents of the UAE are entitled to use the Mobile App, and use of the Mobile App must only occur in the UAE.

6.2 This Data Privacy Policy sets out any consideration regarding our compliance with any required International Data Transfers.

7. Provision of Personal Information and Activation Requirements

7.1 To comply with Applicable Law and to provide, activate, and service your Mobile App and related services, you must provide certain accurate, complete, and up-to-date Personal Data and supporting documents on request. This includes onboarding, KYC/AML checks, activation, funding, ongoing servicing, and periodic reviews.

7.2 Required Information

(i) Identification and contact details (e.g., name, date of birth, nationality, Emirates ID/passport, residential address, email, and mobile number).

(ii) Verification and compliance information (e.g., KYC documents, proof of address, source of funds/source of wealth where applicable).

(iii) Any additional information reasonably requested to meet legal, regulatory, risk, fraud-prevention, or servicing requirements.

7.3 Verification and Screening

(i) We will verify your identity and conduct sanctions, AML/CFT, PEP/adverse media screening and fraud checks, and may obtain information from competent authorities and government-authorized Credit Information Agencies, as permitted by law.

(ii) Where required by law or with your explicit Consent, we may use biometric verification and liveness checks provided via trusted service providers.

7.4 Ongoing Reviews and Re-KYC

(i) We may request updated information or documents at any time, including on a periodic basis or when triggered by risk, legal, or servicing events.

(ii) You must respond within the timeframe we specify; until then, we may place restrictions on your Mobile App or account.

7.5 Accuracy and Updates

(i) You represent and warrant that all information you provide is true, accurate, and not misleading, and you will promptly notify us of any changes (including to your contact details). See "Keeping Your Contact Details Up to Date."

(ii) You authorize us to verify information with third parties and to request or obtain official records as permitted by law.

7.6 Refusal or Failure to Provide Information

(i) If you do not provide required information or fail verification or screening checks, we will be unable to provide or continue to provide the Mobile App or associated services to you.

(ii) We may delay, restrict, suspend, or terminate your Mobile App or account; block or hold Transactions or funds pending review; and refuse loads, reloads, or withdrawals where required by law or risk policy.

(iii) Where legally required, we may file reports with competent authorities (including the FIU) and disclose information to regulators or law enforcement.

7.7 False or Misleading Information

(i) Providing false, inaccurate, or incomplete information is a breach of the Terms and Conditions and may result in immediate suspension or termination.

(ii) We may record this internally and, where permitted or required by law, report to competent authorities and government-authorized Credit Information Agencies.

7.8 Retention of Documents: We will retain copies of identification and verification records for the periods required by law (including at least five (5) years, or longer where legally required for AML/CFT or regulatory purposes).

7.9 If you have questions about information requirements, verification, or activation, please contact Customer Services at +971 600540002 or email to customercare@sharafexchange.com.

8. Keeping Your Contact Details Up to Date

8.1 You must ensure your contact details are accurate and kept up to date at all times so that you receive important notices and communications related to the Mobile App. You agree to notify us without undue delay (and in any event within five (5) business days) of any change to your contact details.

8.2 Changes you must report include: mobile phone number, email address, residential address, mailing address, and any change that may affect delivery of one-time passwords (OTPs) or security alerts.

8.3 How to update: you may update your details through the Mobile App (where available), by contacting our Customer Services (+971 600540002 or customercare@sharafexchange.com), or as otherwise instructed by us. We may require you to complete security verification and provide supporting evidence (e.g., proof of address) before updates take effect.

8.4 Partner-maintained records: where certain records are maintained by any Partner for program administration, you may be required to update your phone number and/or email address directly with the bank (for example, by visiting its branches or using its channels). We will inform you when such Partner updates are required.

8.5 Delivery of communications: to the extent permitted by Applicable Law, notices and service communications will be deemed delivered when sent to the most recent contact details you have provided to us or, where applicable, to the Partner maintaining those records. We are not responsible for any loss arising from your failure to keep your details current or accessible, or from delivery failures caused by your service providers or device settings.

8.6 Security of contact channels: you are responsible for safeguarding access to your phone number, email account, and devices used to access the Mobile App. You must immediately notify us if you suspect SIM-swap, device loss, unauthorized access, or compromise of your email or phone. We may place temporary restrictions on your account until we complete verification.

8.7 Mandatory communications: opting out of marketing does not affect our ability to send you service, security, or legally required communications.

9. Data Retention

We retain Personal Data only for as long as necessary and proportionate to the purposes for which it was collected and as required under Applicable Law. For clarity, "Retention Schedule" means our documented schedule that sets minimum and maximum retention periods by data category, and "Legal Hold" means a suspension of routine deletion triggered by legal, regulatory, or investigatory requirements.

9.1 Retention Criteria

(i) Purpose Limitation: retention is tied to the specific purpose(s) for which Personal Data was collected or subsequently lawfully used.

(ii) Legal/Regulatory Requirements: retention to meet UAE legal obligations (including PDPL and CBUAE regulations and Standards), tax, accounting, AML/CFT, sanctions, chargeback/dispute, and audit requirements.

(iii) Risk and Protection of Rights: retention to establish, exercise, or defend legal claims, for fraud prevention and security, and to protect our rights and the rights of others.

9.2 Minimum Periods (subject to longer periods where required by law or Legal Hold)

(i) Financial, Transactional, and Identity/KYC Records (including consents and related actions): retained for at least five (5) years, or such longer period as may be required by the CBUAE or other competent authorities.

(ii) AML/CFT, Sanctions Screening, and Regulatory Inquiry Records: retained for at least five (5) years and longer where required by law, regulator instructions, or enforcement requests.

(iii) Complaints and Dispute Files (including correspondence and resolutions): retained for at least five (5) years from closure, or longer where required for audits, legal claims, or regulator review.

(iv) Marketing Preferences/Consents and Do Not Contact List entries: retained as long as necessary to honor your preferences and demonstrate compliance with consent/opt-out obligations.

9.3 Post-Closure Retention: Following Mobile App account closure, we continue to retain necessary Personal Data to meet legally imposed record-keeping requirements (including AML/CFT obligations), to resolve disputes, collect debts, respond to regulator or scheme inquiries, and for other lawful purposes described in this Policy.

9.4 Backups and Archives: Where Personal Data resides in system backups or archives, it will be isolated from routine business use and securely overwritten or expired in line with our Retention Schedule and backup rotation cycles, subject to Legal Hold.

9.5 Deletion, Anonymization, and Exceptions

(i) When retention is no longer necessary, we will securely delete Personal Data or irreversibly anonymize it, unless a Legal Hold, regulatory obligation, or legitimate interest (balanced against your rights) requires continued retention.

(ii) Requests for erasure will be honored in accordance with PDPL; however, we may retain data where required to comply with law, regulatory obligations, or to establish, exercise, or defend legal claims.

9.6 Governance and Assurance: We maintain and periodically review our Retention Schedule, keep records of retention decisions, and audit adherence. Third-party Processors are contractually required to apply equivalent retention and secure deletion obligations, including timely return or Deletion at the end of services.

10. Data Security

We implement a risk-based information security program aligned with Applicable Law and industry standards to protect the confidentiality, integrity, and availability of Personal Data and systems all as set out in this Clause 10.

10.1 **Security Governance and Design.** Security-by-design and privacy-by-design principles are applied across systems, products, and processes. Roles and responsibilities for security are defined; staff receive periodic training and awareness. Policies and procedures are reviewed, tested, and updated regularly.

10.2 **Encryption and Key Management.** All Personal Data and Transactional Data are encrypted in transit and at rest using industry-standard protocols. Cryptographic keys are managed securely with restricted access and regular rotation.

10.3 **Access Management.** Access is role-based and granted on a least-privilege, need-to-know basis, with multi-factor authentication for privileged access. Access rights are reviewed periodically and revoked upon role change or termination; access is logged for audit.

10.4 **Network and Application Security.** Segmentation, firewalls, secure configurations, and anti-malware protections are implemented and monitored. Secure Software Development Life Cycle (SSDLC) practices, code reviews, and security testing are applied to applications and the Mobile App.

10.5 **Data Minimization and Protection.** Only the minimum Personal Data necessary for stated purposes is collected and retained. Pseudonymization/Tokenization is used where feasible to reduce risk.

10.6 **Monitoring, Logging, and Vulnerability Management.** We maintain continuous security monitoring, centralized logging, and anomaly detection. Regular vulnerability assessments and periodic penetration testing are performed, with timely remediation tracked to completion.

10.7 **Third-Party and Sub-Processor Controls.** Service Providers and Partners must implement appropriate security measures, process data only on documented instructions, and are subject to audit/assurance as appropriate. Onward disclosure by any third party is prohibited unless permitted by law and contractually authorized with equivalent safeguards. Third parties must

promptly notify us of any Security Incident or Personal Data Breach and cooperate in investigation, mitigation, and notifications.

10.8 **Business Continuity and Disaster Recovery.** Business continuity and disaster recovery plans are maintained, tested periodically, and include backup integrity checks and recovery time objectives appropriate to the services. Backups and archives are protected, access-controlled, and encrypted.

10.9 **Communications Recording.** To provide services, enhance security, and improve quality, telephone calls and certain communications with our contact centers or service teams may be recorded and/or monitored, in accordance with Applicable Law.

10.10 **Security Incidents and Personal Data Breach Notification.** We will assess and respond to Security Incidents promptly. Where a Personal Data Breach may pose a risk to individuals, we will notify the competent authority (including the UAE Data Office where applicable) and affected individuals without undue delay and in accordance with Applicable Law. Notifications will include, to the extent reasonably available: a description of the nature of the breach, likely consequences, measures taken or proposed to address it, and recommended steps individuals can take to mitigate potential adverse effects. We will keep records of Security Incidents and Personal Data Breaches and review lessons learned to improve controls.

10.11 **Account Blocking/Restrictions Notice.** If your account or privileges are blocked or restricted, we will provide written notice within twenty-four (24) hours, including details of the action, required Consumer steps, and contact information, unless prohibited by law or security considerations.

11. Your Rights

11.1 You have the right to access your Personal Data and request corrections (using the contact details in this Privacy Policy).

11.2 You have the right to request erasure of Personal Data where applicable under law (subject to legal/legitimate retention obligations).

11.3 You have the right to request restriction of certain Processing where applicable under law.

11.4 You have the right to object to Processing, including direct marketing; we will stop such Processing unless we demonstrate compelling Legitimate Interests or where required by law.

11.5 You have the right to receive your Personal Data in a structured, commonly used, and machine-readable format and transmit it to another Controller (data portability), where applicable.

11.6 You have the right to withdraw Consent at any time for activities based on Consent (e.g., marketing, non-essential cookies/analytics, and, where required by law, certain International Data Transfers), without affecting the lawfulness of processing before withdrawal. You may also refuse or withdraw Consent to the sharing of Personal Data with Third Parties (noting that refusal may mean we cannot provide the Mobile App or related services).

11.7 You have the right not to be subject to a decision based solely on Automated Decision-Making, including Profiling, that produces legal or similarly significant effects, and to obtain human review, express your point of view, and contest the decision, where required by Applicable Law.

11.8 You have the right to be informed of any directed and repeated attempts of online fraud on your accounts where your identity verification is conducted online.

11.9 You have the right to refuse bundled products or services where you do not wish to obtain all components of such bundle (noting that certain components may be required to operate the Mobile App).

11.10 You have the right to submit a Complaint to us via our complaint management service and escalate to the UAE Data Office (and, where applicable, to the Central Bank of the UAE for Consumer Protection matters). You may contact us at +971 600540002 or customercare@sharafexchange.com, or contact our Data Protection Officer at dpo@sharafexchange.com.

11.11 You have the right to be educated and regularly reminded about how to protect yourself from financial crime, fraud, and cyber risks from time to time.

11.12 **How to exercise your rights:** You may submit a request by contacting us at customercare@sharafexchange.com, or +971 600540002. We will respond within thirty (30) calendar days, and may extend by a further thirty (30) calendar days where requests are complex or numerous, in which case we will notify you of the extension and reasons. We may need to verify your identity and, where permitted by law, may refuse manifestly unfounded or excessive requests or charge a reasonable fee. Certain rights may be limited by Applicable Law, regulatory requirements, legal holds, our record-keeping obligations (including AML/CFT), or the rights of others.

11.13 In addition to the above, you are entitled to request access to Personal Data held about you, if any, by our Mobile App scheme and Partners in connection with the Mobile App. Where appropriate, we will facilitate such requests or direct you to the applicable party. These parties will correct inaccuracies or delete incorrect information that comes to their notice, subject to Applicable Law.

12. Cookies and Website Analytics

12.1 Our Website and App may use cookies, SDKs, and similar technologies (collectively, **"Cookies"** means small files or software components stored on your device or within the App to enable functionality, security, preferences, analytics, and where permitted marketing) to support and improve your experience in accordance with Applicable Law.

12.2 **Purposes.** Subject to your choices, we use Cookies to ensure the Website/App functions securely and as intended (for example, sign-in, session management, and fraud prevention); remember your settings and preferences (for example, language, region, and accessibility); measure user engagement and performance and diagnose issues to improve stability and user experience; and, where permitted by law and with valid Consent, provide and measure marketing and campaign effectiveness.

12.3 **Categories and Consent.** We classify Cookies as follows and apply consent rules consistent with Applicable Law.

12.3.1 Essential for core functionality and security. These do not require Consent.

12.3.2 Remember choices (for example, language). Used with your Consent where required by law.

12.3.3 Help us understand usage to improve services. Used only with your prior Consent.

12.4 **Marketing.** Personalize offers and measure campaigns. Used only with your explicit Consent. We do not use or share Sensitive Personal Data for marketing without your explicit Consent.

12.5 **Your Choices.** You can grant or withdraw Consent for non-essential Cookies at any time through our cookie banner or settings on the Website/App. Withdrawing Consent will not affect the lawfulness of processing before withdrawal, but some features may not function properly if certain Cookies are disabled. For the App, you may also manage device permissions or reset advertising identifiers in your OS settings.

12.6 **Third-Party Tools.** We may use trusted third-party analytics providers (for example, Google Analytics) configured, where available, with privacy-enhancing controls (for example, IP masking). Such providers process data on our behalf under written terms. Any International Data Transfer will follow the safeguards described in this Policy (for example, Adequacy Decisions or Standard Contractual Clauses). We do not combine analytics identifiers with directly identifying data unless permitted by law and necessary for the stated purpose.

12.7 **Retention.** Cookies may be session-based (deleted when you close your browser/App) or persistent (stored until their set expiry or your deletion). We apply proportionate retention and align analytics/marketing data with our Retention Schedule. You may delete Cookies at any time via your browser or device settings.

12.8 **Opt-Out Tools.** You may opt out of Google Analytics by using the browser add-on available at tools.google.com/dlpage/gaoptout and manage ad preferences using your device/browser settings or the tools provided by major platforms.

12.9 **Minors.** We do not knowingly use non-essential Cookies for Minors without the required parental/guardian Consent under Applicable Law.

12.10 **Do Not Track/Global Privacy Controls.** We will assess and, where required by Applicable Law, honor applicable browser or device signals that express your privacy preferences. In any case, you can manage your preferences directly through our cookie banner or settings.

12.11 **Marketing Preferences.** Opting out of marketing Cookies does not affect our ability to send mandatory service or security communications. We maintain a Do Not Contact List to honor your marketing opt-out choices.

13. Marketing and Communication Preferences

13.1 Direct Marketing and Preferences. We will send marketing and promotional communications (e.g., offers, surveys, Program Benefits information) only: (a) with your prior Consent where required by Applicable Law; or (b) as otherwise permitted by Applicable Law. You may withdraw Consent or opt out of marketing at any time, and we will honor your choice without affecting your access to mandatory service communications.

13.2 Channels and Managing Preferences. Subject to your choices, we may contact you via:

13.2.1 SMS, email, in-app/push notifications, or phone; and

13.2.2 other lawful electronic channels you select.

13.3 You can manage or withdraw your marketing preferences at any time through the Mobile App (where available), by contacting Customer Services at +971 600540002 or customercare@sharafexchange.com, or by using the unsubscribe/link or instructions included in our messages. For push notifications, you may also update device/OS permissions.

13.4 Partner Marketing. Where you provide valid Consent (where required by law), our Partners may also use and disclose your Personal Data to:

13.4.1 notify you of related products, services, promotions, and customer surveys;

13.4.2 provide Program Benefits (e.g., loyalty points where applicable); and

13.4.3 conduct research, analytics, product development, service improvement, and planning.

13.5 Any Partner communications will be subject to your preferences and the Partner's own privacy notice. You may withdraw Consent or opt out of Partner marketing at any time using the channels they provide or by contacting us so we can assist.

13.6 Protective Limits. We do not use or share Sensitive Personal Data for marketing without your explicit Consent. We maintain a Do Not Contact List to record and honor opt-outs. We may use limited profiling to tailor marketing only with your Consent where required by law; you have the right to object to such profiling at any time.

13.7 Mandatory Communications. Opting out of marketing does not affect our ability to send service, security, or legally required communications.

13.8 Minors. We do not knowingly engage in direct marketing to Minors without the required parental/guardian Consent under Applicable Law.

13.9 Records. We keep records of Consents and opt-outs and apply suppression for a reasonable period to ensure your choices are respected.

14. Policy Updates

14.1 We may update this Privacy Policy from time to time to reflect changes in Applicable Law, regulatory guidance, our Mobile App operations, or our services and technologies. The "Last Updated" date will appear at the top of the Policy.

14.2 Material changes. Where changes materially affect how we process your Personal Data (for example, new purposes, new categories of recipients, or changes to your rights), we will provide prior notice where required by law via one or more of: email, SMS, in-app/push notification, or notice on our Website/App. Such changes will take effect on the date stated in the notice. Where the law requires your Consent (for example, certain marketing or international transfers), we will obtain it in advance; otherwise, your continued use of our services after the effective date constitutes acceptance of the updated Policy.

14.3 Non-material changes. Clarifications, formatting, and administrative updates that do not change how we process your Personal Data will be effective upon posting on our Website/App.

14.4 Version control and access to prior versions. We will maintain version control and make prior versions available upon request. You are encouraged to review this Policy periodically.

14.5 Languages. This Privacy Policy is available in English and Arabic. Both versions are intended to be consistent; however, if there is any inconsistency, the English version shall prevail to the extent permitted by Applicable Law.

14.6 Questions about updates. If you have questions about this Policy or any updates, please contact us at +971 600540002, customercare@sharafexchange.com, or our Data Protection Officer at dpo@sharafexchange.com.

15. Governing Law and Jurisdiction

This Privacy Policy is governed by the laws of the United Arab Emirates as applicable in the Emirate of Dubai, without regard to conflict-of-law principles. Any dispute arising out of or in connection with this Privacy Policy shall be subject to the non-exclusive jurisdiction of the Courts of Dubai. You and Sharaf Exchange irrevocably submit to such jurisdiction and waive any objection to venue or forum non conveniens. Nothing in this clause limits Sharaf Exchange's right to seek interim, injunctive, or conservatory relief in any competent court.

16. Terms and Conditions

For detailed information on how the Mobile App services operate (including features, fees, limits, and your obligations), please refer to our Terms and Conditions. The Terms and Conditions govern the provision and use of the Mobile App, while this Privacy Policy governs how we collect, use, and protect your Personal Data.

17. Complaints

You may submit a complaint through Customer Services at +971 600540002 or by email to customercare@sharafexchange.com. For privacy-related complaints, you may also contact our Data Protection Officer at dpo@sharafexchange.com.

We will acknowledge your complaint promptly and provide a response within thirty (30) calendar days. If your complaint is complex or involves multiple issues, we may extend this period by up to an additional thirty (30) calendar days and will notify you of the extension and the reasons.

Please include your full name, contact details, a brief description of the issue, relevant dates, and any supporting documents to help us investigate efficiently. If you are not satisfied with our response, you may escalate to the UAE Data Office (for data protection matters) and, where applicable, the Central Bank of the UAE for Consumer Protection matters.

18. **If you confirm, I'll perform the cleanup in one pass and keep all substantive content intact. Contact Us**

    If you have any questions, concerns, or complaints regarding this Privacy Policy or your Personal Data, please contact us using the details below.

    Sharaf Exchange LLC
    Customer Services: +971 600540002
    Email (General): customercare@sharafexchange.com
    Data Protection Officer: dpo@sharafexchange.com
    Website: www.sharafexchange.ae