PRIVACY POLICY

UNIQUNITS Mobile Application Effective date: May 5, 2026 **Version:** 1.0

---

1. GENERAL PROVISIONS

1.1. Who we are

This Privacy Policy (the "**Policy**") is issued by **UNIQ LAB FZCO** (the "**Company**", "**we**", "**us**", "**our**"), a free zone company incorporated under the laws of the United Arab Emirates, with its registered office at IFZA Business Park, DDP, PO Box 342001, Dubai, United Arab Emirates, License No. 52386, Registration No. DSO-FZCO-50056.

The Company acts as the **data controller** in respect of personal data collected through the UNIQUNITS mobile application (the "**Application**"), the website www.uniqunits.com (the "**Website**") and any related services (collectively, the "**Services**").

1.2. Scope of this Policy

This Policy applies to all natural persons who: - download, install or use the Application; - visit the Website; - register an account or create a partner account; - purchase a Subscription or use the Trial period; - otherwise interact with the Company in connection with the Services.

1.3. Acknowledgement

By using the Services, you confirm that you have read and understood this Policy. Where required by applicable law, processing is carried out only on the basis of your separate consent, a contract, our legal obligations or a legitimate interest, as set out in Section 3.

1.4. Applicable law

We process personal data in accordance with: - **UAE Federal Decree-Law No. 45 of 2021** on the Protection of Personal Data ("**UAE PDPL**") and its Executive Regulations; - **Regulation (EU) 2016/679** ("**GDPR**") and the **UK GDPR**, where applicable to data subjects located in the EEA / United Kingdom; - the **California Consumer Privacy Act** ("**CCPA / CPRA**"), where applicable to California residents; - any other data-protection law applicable to a specific user based on their location.

---

2. PERSONAL DATA WE COLLECT

2.1. Data you provide directly

Category	Examples
Identity & contact data	full name, email address, Billing region
Account data	username, password (stored as a hash), profile picture (optional), language

Category	Examples
	preferences
Payment data	billing name, billing country, transaction reference, subscription status (full card data is processed exclusively by our payment providers — see Section 5)
Educational data	progress in the educational module, test answers, score, certificate ID and issuance date
Communications	support requests, complaints, feedback, correspondence with us
KYC / Partner data (Partners only)	identity documents, tax residency, payment account details, corporate documents — where the user joins the Affiliate Program

2.2. Data collected automatically

Category	Examples
Device & technical data	device model, operating system, unique device identifier (advertising ID where consented to), language, time zone, crash logs
Usage data	screens viewed, features used, session duration, frequency of use, in-app actions
Network data	IP address (truncated where possible), approximate geographic location derived from IP, internet service provider
Cookies & SDKs	as further described in our **Cookie Policy**

2.3. Data from third parties

We may receive data from: - **payment processors** (transaction status, transaction ID, anti-fraud signals); - **app stores** (Google Play, Apple App Store) — install, update, uninstall, in-app purchase events; - **analytics and attribution providers** — aggregated usage and campaign data; - **affiliate / referral partners** — referral identifier, click ID; - **identity-verification or anti-fraud providers** — verification result (pass / fail), risk score.

2.4. Data we do not intentionally collect

- Full payment-card numbers, CVV/CVC codes — these are entered directly into our payment provider's PCI-DSS compliant interface;
- Biometric data;
- Special categories of personal data under Art. 9 GDPR / Art. 15 UAE PDPL (e.g. health, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, trade-union membership);
- Personal data of children under 18;
- Trading data executed via third-party broker platforms.

If special-category data is provided to us by mistake, we will delete it without undue delay.

3. PURPOSES AND LEGAL BASES OF PROCESSING

3.1. Lawful bases

We process personal data only where one or more of the following lawful bases applies. Where the GDPR / UK GDPR applies, the bases listed in Art. 6(1) GDPR apply; where the UAE PDPL applies, the equivalent bases under Art. 4 UAE PDPL apply.

Purpose	Categories of data	Legal basis
Creating and operating your account; providing the Application and educational module	Identity, account, educational data	Performance of a contract (Art. 6(1)(b) GDPR / Art. 4 PDPL)
Processing payments and Subscriptions	Payment data, account data	Performance of a contract; legal obligation (accounting, tax)
Issuing and verifying Certificates	Educational data, identity	Performance of a contract
Customer support and complaint handling	Communications, account	Performance of a contract; legitimate interest
Security, fraud prevention, abuse detection	Device, network, usage, account	Legitimate interest; legal obligation
Analytics and product improvement	Usage, device data (aggregated where possible)	Legitimate interest; consent (where required by ePrivacy)
Marketing communications and personalization	Identity, contact, usage	**Consent** (Art. 6(1)(a) GDPR); soft opt-in for existing customers where permitted
AML, sanctions screening, KYC (mainly Partners)	Identity, payment, KYC documents	Legal obligation; legitimate interest
Compliance with legal requests, defence of claims	All categories as required	Legal obligation; legitimate interest
Cross-border data transfers	All categories as required	Appropriate safeguards under Art. 46 GDPR / UAE PDPL Art. 22–23

Where we rely on **legitimate interests**, we have carried out a balancing test and you have the right to object as set out in Section 6.

3.2. Marketing and consent management

We send marketing communications only: - with your **prior, freely given, specific, informed and unambiguous consent**, where such consent is required (e.g. EEA, UK); or - on the basis of a soft opt-in for existing customers regarding similar products, where permitted by law.

You may withdraw consent or unsubscribe at any time, free of charge, by: - clicking the "Unsubscribe" link in any marketing email; - changing notification settings in the Application; - emailing us at **info@uniqunits.com**.

Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

---

4. DATA STORAGE, SECURITY AND RETENTION

4.1. Hosting and cross-border transfers

Personal data may be hosted on servers located in the United Arab Emirates, the European Union and other jurisdictions where our service providers operate. Where data is transferred outside the country of the data subject, we ensure an adequate level of protection through one or more of the following mechanisms: - transfer to a country recognized as providing an adequate level of protection (Art. 45 GDPR / Art. 22 UAE PDPL); - **Standard Contractual Clauses** ("SCCs") issued by the European Commission, supplemented where required by additional safeguards (Schrems II); - **UK International Data Transfer Agreement** (or UK Addendum to the SCCs); - approved binding corporate rules, certifications or codes of conduct; - explicit consent of the data subject under derogations of Art. 49 GDPR / equivalent UAE rules, where applicable.

A copy of the relevant transfer mechanism may be requested at info@uniqunits.com.

4.2. Security measures

We implement appropriate technical and organizational measures, including: - TLS / SSL encryption of data in transit; - encryption at rest for sensitive credentials and KYC documentation; - access control on a least-privilege basis with multi-factor authentication for administrators; - secure password storage (salted hashing); - network segmentation, firewalling and logging; - regular security testing, vulnerability scanning and patching; - data backups and disaster recovery procedures; - staff confidentiality obligations and data protection training; - incident response procedures, including the obligation to notify the competent supervisory authority within 72 hours of becoming aware of a personal data breach where required by GDPR Art. 33, and in line with UAE PDPL Art. 9.

No system is fully secure. If you have reason to believe your data has been compromised, please contact us immediately at info@uniqunits.com.

4.3. Retention periods

We retain personal data only for as long as necessary for the purposes described in this Policy:

Category	Retention period
Account data	While the account is active and for **2 years** after deletion (to handle disputes, fraud and chargebacks)
Subscription / payment / accounting data	**5 years** from the date of the transaction (UAE Commercial Companies Law and tax

Category	Retention period
	requirements; up to **10 years** where local accounting law requires)
KYC / AML records (Partners)	**5 years** after the end of the relationship, in line with UAE Federal Decree-Law No. 20 of 2018 on AML
Educational data and Certificates	While the account is active and for up to **3 years** after deletion (for verification of issued Certificates)
Marketing data	Until withdrawal of consent; suppression list kept indefinitely to ensure unsubscribe is honoured
Server logs, security events	**12 months** as a default
Correspondence and complaints	**3 years** from closure
Cookies / SDK identifiers	As stated in the Cookie Policy

After expiry of the relevant period, data is deleted or irreversibly anonymized.

---

5. SHARING PERSONAL DATA WITH THIRD PARTIES

5.1. Categories of recipients (data processors)

We share personal data only with carefully selected providers, bound by written data-processing agreements imposing GDPR Art. 28 / UAE PDPL Art. 26 obligations. Categories include: - cloud hosting and infrastructure providers; - payment processors and payment gateways; - analytics and attribution providers; - email, push-notification and customer-support providers; - crash-reporting and performance-monitoring providers; - anti-fraud and identity-verification providers; - professional advisers (lawyers, auditors, accountants).

A current list of sub-processors is available upon request.

5.2. Disclosures required by law

We may disclose personal data: - to competent authorities, regulators, courts or law-enforcement bodies, where legally required; - to protect our rights, property and safety or those of our users or the public; - in connection with the prevention, detection or investigation of fraud, money laundering, terrorist financing or other unlawful activity.

5.3. Corporate transactions

In a merger, acquisition, financing, reorganization, insolvency or sale of all or part of our business, personal data may be transferred to the relevant counterparty subject to confidentiality undertakings and the protection level of this Policy. Affected users will be informed where required by law.

5.4. No sale of personal data

We do not sell personal data for monetary or other valuable consideration, as defined under the CCPA/CPRA, and we do not engage in cross-context behavioral advertising.

---

6. YOUR RIGHTS

6.1. Rights of data subjects

Subject to applicable law and identity verification, you may exercise the following rights: - **Right to information and access** – obtain confirmation whether we process your data and a copy of it; - **Right to rectification** – correct inaccurate or incomplete data; - **Right to erasure / right to be forgotten** – obtain deletion of your data in certain cases; - **Right to restriction of processing**; - **Right to data portability** – where processing is based on consent or contract and is automated; - **Right to object** – including to processing based on legitimate interests and to direct marketing at any time; - **Right not to be subject to a decision based solely on automated processing** producing legal or similarly significant effects; - **Right to withdraw consent** at any time without affecting prior lawful processing; - **Right to lodge a complaint** with a competent supervisory authority — in the UAE, the **UAE Data Office**; in the EEA, your local Data Protection Authority; in the UK, the **Information Commissioner's Office (ICO)**.

CCPA/CPRA-specific rights (right to know, delete, correct, opt out of sale/sharing, limit use of sensitive personal information, non-discrimination) are honoured for California residents.

6.2. How to exercise your rights

Send a request to **info@uniqunits.com**, specifying: - your full name and the email address registered with the account; - the right(s) you wish to exercise; - supporting information sufficient to identify you.

We will respond within **30 calendar days** (extendable by up to 60 days for complex or numerous requests; you will be notified of any extension). Requests are free of charge unless manifestly unfounded or excessive.

6.3. Identity verification

To prevent unauthorized access we may take reasonable steps to verify the requester's identity (for example, a confirmation email from the registered address). We will not disclose data to a person who cannot be reasonably identified as the data subject.

---

7. COOKIES AND SIMILAR TECHNOLOGIES

Our use of cookies, SDKs, pixels, local storage and similar technologies is described in our separate **Cookie Policy**, which forms an integral part of this Privacy Policy. Where required by law (in particular ePrivacy and GDPR), non-essential cookies are set only after the user's prior, freely-given consent obtained via our cookie consent banner.

---

8. CHILDREN

The Services are intended exclusively for persons aged **18 years or above**. We do not knowingly collect personal data from minors. If we become aware that we have collected data from a person under 18 without verifiable parental consent, we will delete such data promptly. Parents or guardians may contact us at info@uniqunits.com.

---

9. AUTOMATED DECISION-MAKING AND PROFILING

We do **not** carry out fully automated decisions producing legal or similarly significant effects on users (Art. 22 GDPR). Where we use automated tools for fraud prevention or eligibility checks (e.g. AML screening of Partners), a human review is available upon request.

---

10. CHANGES TO THIS POLICY

We may update this Policy from time to time. **For material changes, we will notify Users via the Application and/or by email at least 14 calendar days before the changes become effective.** The current version is always available within the Application and on the Website. Continued use of the Services after the effective date constitutes acceptance of the updated Policy. If you do not agree, you must stop using the Services and may delete your account.

---

11. CONTACT DETAILS AND DATA PROTECTION OFFICER

Data Controller: UNIQ LAB FZCO IFZA Business Park, DDP PO Box 342001, Dubai, United Arab Emirates License No. 52386 | Registration No. DSO-FZCO-50056

Privacy / Data-Protection contact: Email: **info@uniqunits.com** Subject line: “Privacy Request” Website: www.uniqunits.com

For users located in the European Union or the United Kingdom, an EU/UK representative under Art. 27 GDPR / UK GDPR may be appointed; the relevant contact details will be published on our Website once appointed.

This Privacy Policy forms an integral part of the UNIQUNITS Terms of Service.