GUARDIAN AI PRIVACY NOTICE

Last Updated: November 6, 2025

Effective Date: November 6, 2025

Introduction

Welcome to Guardian AI for Innovation & Artificial Intelligence Research & Consultancies L.L.C., committed to protecting personal data in line with UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL).

This Privacy Notice explains how Guardian AI (we, us, our) collects, uses, shares, stores, and protects personal data when the Guardian AI mobile application (the App) is used.

By using the App, acknowledgment is provided that the data practices described herein have been read, understood, and accepted.

Controller information and contact

Data Controller

Guardian AI for Innovation & Artificial Intelligence Research & Consultancies L.L.C.
Business Bay, Citadel Tower - 2106, Dubai, United Arab Emirates
Phone: +971585872409

Data Protection Officer (DPO)

For high-risk processing activities (systematic monitoring and automated profiling), Guardian AI designates a contact point for privacy and data protection matters.

Email: support@guardianai.info (use subject "PDPL Rights Request" or "Privacy Inquiry")

Contact for privacy

- **General privacy inquiries**: support@guardianai.info

- **Data subject rights requests**: support@guardianai.info
- **Security incidents**: support@guardianai.info
- **Rewards Program disputes**: support@guardianai.info (subject: "Rewards Dispute")

Response time: within 30 days as required by Article 26 of UAE PDPL, with any justified extension communicated in writing. Rewards Program disputes receive responses within 14 business days.

Scope and application

Territorial scope

This Notice applies to users of the App within the United Arab Emirates, to processing of UAE residents' personal data regardless of processing location, and to cross-border transfers of UAE-origin data.

Regulatory framework

Compliance includes UAE PDPL for Onshore UAE users, DIFC Data Protection Law 2020 where applicable, ADGM Data Protection Regulations 2021 where applicable, TDRA IoT Policy requirements, and CBUAE consumer protection requirements for insurance-related data sharing.

Personal data collected

Identifiers and account information

Collected data may include full name, email address, optional phone number, date of birth, optional driver's license number, device identifiers (UDID, Advertising ID, IDFV), hashed credentials, and optional profile photo.

Location data (continuous and precise)

Data includes real-time GPS coordinates, continuous trip traces, route history and patterns, geocoded addresses, and supplemental cell/Wi-Fi positioning, collected continuously while the

App detects driving, during manually started trips, and when background location permission is granted.

Background collection continues when the App is not on screen and requires "Always Allow" permission for automatic trip detection.

Motion and sensor data

Accelerometer, gyroscope, and magnetometer data are collected to derive events such as harsh braking, rapid acceleration, swerving, and impact detection, sampled at approximately 10–100 Hz during driving.

Vehicle telemetry data (if OBD-II connected)

If an OBD-II adapter is connected, additional telemetry such as VIN, RPM, throttle, coolant temperature, fuel metrics, DTCs, voltage, oxygen readings, and vehicle speed may be collected, with OBD-II remaining optional and core functionality available via smartphone sensors.

Device and technical data

Device type and model, OS version, App version, IP and network info, carrier, language, timezone, battery and charging status, and available storage may be collected to support App performance and background operations.

Usage and analytics data

App launches, session duration, feature interactions, screens viewed, queries, crash logs, and performance metrics may be collected for reliability and improvement.

Derived and inferred data (profiling)

Automated processing generates safety scores, sub-scores, risk classifications, incident probability estimates, behavioral patterns, and coaching recommendations, which may affect opt-in insurance quotes, gamification, or access to discounts.

Rewards Program data

Data collected and processed specifically for the Guardian AI Rewards Program includes:

- **Points Accumulation**: Per-trip points calculated from safety scores, monthly point totals, and historical point trends
- **Voucher Information**: Generated voucher values, issuance dates, redemption status, expiration dates, and redemption history
- **Competition Data**: Queen Bee competition rankings, monthly leaderboard positions, and winner determinations
- **Redemption Transactions**: Payout requests, processing status, payout amounts, email confirmations, and transaction timestamps
- **Anti-Fraud Metadata**: Trip pattern analysis, device integrity checks, behavioral anomaly flags, and fraud risk scores

This data is displayed in the **Rewards tab** on a per-trip basis and used to calculate monthly rewards, determine competition winners, process redemptions, and detect fraudulent or gaming behavior.

Sensitive data

No biometric or health data is currently collected, while location data may reveal sensitive places and behavioral patterns and is handled with minimization and pseudonymization; future opt-in biometrics or health features would require separate consent, granular controls, stricter retention, and enhanced encryption.

Data not collected

Audio content, contact lists, media library content (except an optional profile photo), messages or emails, browsing history outside the App, and payment card numbers are not collected, with platform stores processing payments.

How data is collected

Direct collection

Account forms, profile settings, in-app surveys, support communications, opt-in insurance consent forms, and Rewards Program redemption requests may be used to collect data.

Automatic collection

GPS, motion sensors, optional OBD-II via Bluetooth, analytics/crash reporting SDKs, and automated rewards points calculation facilitate automatic collection.

Third-party sources

Mapbox supports mapping and geocoding, Apple/Google may provide in-app purchase metadata and device identifiers, and insurance partners may be used for policy verification and rewards redemption processing with explicit consent.

Lawful bases for processing

Consent (Article 5(1)(a))

Explicit consent is required for insurance sharing, "Always Allow" background location collection, marketing communications, and Rewards Program participation with insurance partner coordination, and may be withdrawn via device settings, in-app privacy settings, or by emailing support@guardianai.info with "Withdraw Consent" in the subject, noting that core functionality and Rewards Program eligibility may be limited if location or sensor permissions are withdrawn.

Contract performance (Article 5(1)(b))

Processing to deliver trip recording, scoring, event detection, navigation, account support, and Rewards Program services (points calculation, voucher generation, competition rankings, redemption processing) is necessary for core App functionality.

Legal obligation (Article 5(1)(c))

Compliance with TDRA, judicial or regulatory orders, tax or record-keeping (including 7-year retention of redemption transactions for tax purposes), and age verification obligations provide a lawful basis.

Legitimate interests (Article 5(1)(d))

Fraud prevention (including Rewards Program gaming detection), service improvement, safety research, network security, Rewards Program integrity, and legal defense are pursued with documented DPIAs, and objections may be raised under Article 18 as described below.

How data is used

Core service delivery

Trip recording, safety scoring, event detection, coaching, navigation, and progress tracking are core to the App's purpose.

Rewards Program operations

Personal data is used to:

- **Calculate Points**: Automatically calculate and display points on a per-trip basis in the Rewards tab based on driving safety scores
- **Generate Vouchers**: Create monthly vouchers worth up to 25% of monthly insurance premium (annual premium ÷ 13) based on accumulated points
- **Determine Competition Winners**: Identify the monthly Queen Bee winner for 100% monthly insurance premium cashback
- **Process Redemptions**: Handle manual user-initiated voucher redemption requests with 7 business day payout and email confirmation
- **Detect Fraud**: Monitor for GPS spoofing, impossible trip patterns, device manipulation, score manipulation, and other prohibited gaming activities
- **Enforce Program Rules**: Apply consistent anti-fraud measures, investigate disputes, and process appeals with human review

Processing for rewards relies on contract performance (to deliver the rewards service you've opted into), consent (for insurance partner coordination where applicable), and legitimate interests (fraud prevention and program integrity) as lawful bases under UAE PDPL Article 5.

Automated profiling and decisions

Automated algorithms calculate scores, classify risk, generate coaching, detect anomalies, calculate rewards points, determine Queen Bee winners, and identify fraud patterns, which may influence opt-in insurance offers, in-app rewards eligibility, leaderboards, voucher values, and competition rankings, with rights to human review, explanation, contestation, and opt-out

as described, exercisable in-app (Rewards tab > Help & Support > Dispute) or via support@guardianai.info.

Significant Effects: Automated rewards decisions may affect insurance premium benefits, competition prizes, and account sanctions for suspected fraud.

Analytics and improvement

Bug detection, A/B tests, usage analysis, ML model improvements, and rewards algorithm optimization are conducted to enhance reliability and user value.

Communications

Transactional notifications (including trip points, voucher generation, competition results, redemption confirmations, and expiration reminders) are necessary for the service, while promotional messages require opt-in and may be withdrawn at any time.

Safety and security

Fraud detection (including Rewards Program gaming), Terms enforcement, threat protection, and legal compliance are supported by appropriate data use.

Research and aggregated insights

Anonymized statistics and safety research, including aggregated rewards participation metrics, may be published or shared once data can no longer reasonably identify individuals under PDPL standards.

Data sharing and disclosure

Service providers (processors)

- **Google Cloud Platform** provides cloud storage, compute, and ML, receiving relevant categories of personal data (including rewards data) under SCCs and encryption controls in selected global regions.
- **Flespi** provides MQTT message brokerage for real-time telematics streaming with encrypted transport and limited retention.

- **Mapbox** supports mapping, geocoding, and routing using temporary location inputs and telemetry consistent with its published privacy practices.
- **Firebase** supports analytics, crash reporting, performance monitoring, and push notifications with data minimization, encryption, and set retention windows.

Insurance partners (opt-in only)

With separate explicit consent and when participating in the Rewards Program, aggregated scores, trip summaries without raw GPS, risk classification, and de-identified patterns may be shared, along with:

- **Redemption Activity**: Voucher redemption history and cashback payout records to validate premium adjustments
- **Competition Results**: Queen Bee winner status for cashback processing
- **Fraud Alerts**: Flagged accounts with suspected gaming or manipulation (to protect insurance partner interests)

Insurance partners process redemptions and cashbacks as independent controllers, with in-app controls to opt-in, revoke, and view sharing history, and insurers making independent underwriting decisions.

Business transfers

In a merger, acquisition, sale, bankruptcy, or liquidation, data (including unredeemed rewards) may transfer to a successor entity under consistent protections with notice and an opportunity to object or request deletion before transfer where feasible.

Legal and regulatory disclosures

When required by law, data may be disclosed for court orders, regulatory inquiries, legal claims, or imminent harm prevention, with notice where not legally prohibited, scope minimization, and challenges to overbroad requests.

Aggregated and anonymized data

Anonymized, aggregated insights that cannot identify individuals, including rewards program statistics (average points earned, redemption rates, competition participation), may be shared publicly or with partners for research and benchmarking.

Cross-border data transfers

Why data is transferred

Global cloud and telematics services enable reliability, scalability, and advanced AI/ML capabilities beyond UAE-only infrastructure, including rewards calculation algorithms and fraud detection systems.

Legal basis (PDPL Article 43)

Approved contractual clauses are executed with processors, adequate jurisdiction assessments favor robust regimes and certified providers, and technical safeguards such as TLS 1.3, AES-256, pseudonymization, and RBAC are implemented, supported by documented Transfer Risk Assessments.

Your explicit consent

Use of the App and participation in the Rewards Program constitute explicit consent to described cross-border transfers, with the option to discontinue use and request deletion if consent is withdrawn.

Data retention and deletion

Retention principles

Data is retained only as necessary for service delivery, legal obligations (including tax compliance for redemption transactions), and legitimate interests with pseudonymization and anonymization applied over time.

Retention periods by category

Data Category	Retention Period	Post-Retention Action

Raw GPS Traces	365 days after trip	Deleted (no backup)
Motion Sensor Data	365 days after trip	Deleted (no backup)
Aggregated Trip Summaries	24 months	Pseudonymized, then anonymized after 36 months
Safety Scores & Trends	24 months	Pseudonymized, then anonymized after 36 months
Per-Trip Rewards Points	**24 months after trip**	**Deleted (aggregated monthly totals retained)**
Monthly Points Totals	**36 months**	**Anonymized for analytics**
Voucher Records	**12 months after expiry/redemption**	**Deleted (except aggregated statistics)**
Queen Bee Competition Results	**36 months**	**Anonymized for historical records**
Redemption Transactions	**7 years (tax/audit compliance)**	**Deleted or fully anonymized**
Fraud Investigation Records	**5 years after case closure**	**Deleted (except for legal holds)**

Account Information	Until account deletion + 30 days	Deleted; backups purged within 90 days
OBD-II Telemetry	12 months	Deleted
Support Tickets	36 months after resolution	Deleted (except anonymized training data)
Crash Logs	Until resolution (max 12 months)	Deleted
Anonymized Aggregate Data	Indefinitely	Not re-identifiable

Pseudonymization, anonymization, and backups

User identifiers may be replaced with hashes before full anonymization, and production backups and disaster recovery archives follow 30–90 day cycles with deletion requests purged from backups within 90 days.

Early deletion

Deletion may be requested at any time and is completed within 30 days unless legal holds, payment disputes, mandatory tax retention, or mandatory retention apply. **Unredeemed rewards vouchers are forfeited upon account deletion without compensation.**

Data security measures

Technical safeguards

TLS 1.3 in transit, AES-256 at rest, customer-managed backup encryption keys, secure keychains on devices, RBAC, MFA, audit logging, JIT access, VPC firewalls, DDoS protection, IDS, API rate limiting, secure coding, dependency scanning, penetration testing, and optional bounty programs support defense-in-depth.

Organizational safeguards

Annual privacy and security training, confidentiality agreements, vendor due diligence and contractual controls, and an incident response plan with regulator notification within 72 hours for qualifying breaches and prompt user notice where high risk exists are maintained.

Certifications and limitations

Industry certifications are targeted and inherited where applicable, recognizing that no system is 100% secure and encouraging strong passwords, updates, and prompt reporting to support@guardianai.info.

Your rights under UAE PDPL

Right of access (Article 15)

Request a copy of personal data (including Rewards Program data such as points history, voucher records, redemption transactions) via in-app export or support@guardianai.info, generally within 30 days in a machine-readable format, with reasonable fees only for excessive requests.

Right to rectification (Article 16)

Correct inaccuracies in-app or by contacting support@guardianai.info, with timely resolution and identity verification where appropriate.

Right to erasure (Article 17)

Delete the account and data via in-app controls or support@guardianai.info, completed within 30 days and backups within 90 days, subject to legal exceptions. **Note**: Deletion of account data results in forfeiture of all unredeemed rewards vouchers without compensation.

Right to object (Article 18)

Object to processing based on legitimate interests by emailing support@guardianai.info, with assessment in 14 days and processing halted absent compelling grounds, noting possible feature impact. You may specifically object to:

- **Automated profiling for Rewards Program purposes**
- **Points calculation algorithms**
- **Fraud detection and gaming prevention measures**
- **Queen Bee competition eligibility determinations**

Objecting to Rewards Program profiling will result in disqualification from the Rewards Program while maintaining core driving analytics functionality.

Right to restrict (Article 19)

Request temporary suspension during disputes or legal needs, with storage without processing until restrictions are lifted with notice.

Right to data portability (Article 20)

Receive data (including rewards history) in structured, machine-readable form within 14 days via secure download for data provided or generated through use.

Right to withdraw consent (Article 8)

Revoke consent via device or in-app settings or by emailing support@guardianai.info, without retroactive effect and with potential impact on core functionality and Rewards Program eligibility.

Right to lodge a complaint (Article 44)

Concerns may be raised first with support@guardianai.info and then, if needed, with the relevant UAE authority, the DIFC Commissioner of Data Protection, or ADGM Registration Authority, as applicable.

For Rewards Program disputes specifically, use the in-app dispute process (Rewards tab > Help & Support > Dispute) or email support@guardianai.info with subject "Rewards Dispute" before escalating to regulatory complaints.

Special considerations

Children's privacy

The App is not intended for users under 18, with verification at registration and immediate deletion upon discovery of minor data, and guardian requests honored with proof.

Automated trip detection

Driving is inferred from speed, GPS patterns, and sensor analysis, with possible false positives for passengers and in-app controls to disable auto-detection, delete trips, or mark Passenger Mode. **Points are calculated based on trip data quality**. Trips with poor GPS accuracy, insufficient duration (<5 minutes), or minimal distance (<2 km) may not qualify for points. Manually deleted trips or trips marked as "Passenger Mode" do not earn points.

Battery and data usage

Continuous location and sensors impact battery and data, mitigated by adaptive sampling and battery-aware processing, with options such as Wi-Fi-only uploads.

Insurance data sharing (opt-in)

Prior disclosure, explicit consent, no adverse impact for refusal, independent insurer control as controller, and active consent management are provided.

Rewards Program specific considerations

Voluntary participation

Participation in the Guardian AI Rewards Program is entirely voluntary. You may opt out at any time by discontinuing rewards redemption, though historical points and voucher data will be retained per the schedules above.

Automated decision-making with significant effects

The Rewards Program uses automated algorithms that may produce significant effects:

- **Voucher Value Determination**: Algorithms calculate voucher amounts based on monthly points
- **Queen Bee Winner Selection**: Automated ranking determines competition winners
- **Fraud Sanctions**: Automated fraud detection may result in account suspension or rewards forfeiture

In accordance with UAE PDPL Article 18, you have the right to:

- Request **human review** of any automated decision by emailing support@guardianai.info with subject "Rewards Appeal"
- Receive **meaningful explanation** of the logic, factors, and significance of automated processing
- **Contest outcomes** through our in-app dispute resolution process (Rewards tab > Help & Support > Dispute)
- Receive a response to appeals within **21 business days**

Anti-fraud transparency

We employ multiple anti-fraud measures to ensure fair program operation:

- GPS integrity validation and motion sensor consistency checks
- Detection of device manipulation (jailbreaking, rooting, GPS spoofing)
- Behavioral pattern analysis and anomaly detection using machine learning
- Statistical modeling to identify impossible or improbable trip patterns

Fraud determinations are made fairly and consistently across all users. False positives may occur; you have the right to appeal with evidence.

Tax implications

Rewards (vouchers, cashback) may constitute taxable income under UAE law. You are solely responsible for reporting and paying any applicable taxes. We may report reward values to UAE tax authorities as required by law. Consult a tax professional for guidance.

Voucher expiration and forfeiture

- Vouchers expire **12 months** from issuance date
- Expired vouchers are forfeited with no compensation or extension
- The App will send expiration reminders 30 days and 7 days in advance
- Unredeemed vouchers at account deletion are forfeited without refund

Insurance partner dependency

Voucher redemption and Queen Bee cashback depend on active partnerships with insurance providers. If a partner relationship terminates, we will offer reasonable alternative redemption options or pro-rata compensation, but are not obligated to do so under UAE law.

Cookies and tracking technologies

Mobile identifiers and SDKs

IDFV/Android ID, resettable advertising IDs, Firebase Analytics, and Crashlytics may be used for analytics, reliability, and fraud detection with in-app privacy toggles.

Local storage and sandboxing

Preferences, caches, credentials, and rewards data may be stored locally via secure platform stores, accessed only by the App under OS sandboxing.

Third-party tracking

No ad networks, social pixels, or cross-app tracking are integrated, and Mapbox collects anonymized telemetry as part of mapping features per its published policy.

International users

Primary jurisdiction: UAE

This Notice is designed for UAE PDPL compliance, and use from outside the UAE is processed under UAE law.

Additional rights (EU/UK)

GDPR/UK GDPR rights, including limits on automated decisions and enhanced consent standards, may apply, with representative details provided if appointed.

California privacy rights

California residents may exercise rights to know, delete, and opt-out of "sale" or "sharing," noting that Guardian AI does not "sell" personal information as defined, and requests can be sent to support@guardianai.info.

Data Protection Impact Assessment (DPIA)

High-risk processing

DPIAs cover continuous GPS monitoring, automated profiling with significant effects (including rewards determinations), large-scale sensitive location processing, and cross-border transfers.

Conclusions and availability

Processing is necessary and proportionate with minimization and safeguards, residual risks are low, and summaries can be requested from support@guardianai.info.

Changes to this Privacy Notice

Right to modify

Updates may reflect legal changes, new features (including Rewards Program modifications), feedback, or security enhancements.

Notice of material changes

Material updates will be communicated through in-app banners, email, push notifications, and version history with at least 30 days' notice where feasible.

Continued use and disagreement

Continued use after changes signifies acceptance, and discontinuation and deletion may be requested if disagreement persists.

Version control

Current Version: 1.1; **Last Updated and Effective Date: November 6, 2025**; prior versions may be archived for reference.

Contact us

Company and address

Guardian AI for Innovation & Artificial Intelligence Research & Consultancies L.L.C., Business Bay, Citadel Tower - 2106, Dubai, United Arab Emirates.

Email and phone

Support and privacy contact: support@guardianai.info; Phone: +971585872409.

Security incidents

Report suspected incidents to support@guardianai.info for immediate triage and follow-up per incident response procedures.

Acknowledgment and consent

By using the App and participating in the Rewards Program, it is acknowledged that:

- Continuous, precise location data may be collected while driving and used for points calculation
- Automated profiling may have significant effects on rewards eligibility, voucher values, and competition rankings
- Cross-border transfers occur under safeguards described in this Notice

- Rights under UAE PDPL are understood, including the right to human review of automated rewards decisions
- Consent may be withdrawn at any time with potential functional limitations, including **disqualification from the Rewards Program**
- Rewards (vouchers, cashback) may have tax implications that are the user's sole responsibility
- Unredeemed vouchers are forfeited upon account deletion

If consent is not provided, the App should not be used, or you may disable Rewards Program participation in Settings > Rewards > Opt Out.

Appendix A: Glossary

Definitions include personal data, sensitive data, processing, controller, processor, pseudonymization, anonymization, profiling, cross-border transfer, SCCs, and DPIA as used in this Notice.

Appendix B: Privacy rights quick reference

Right	What It Means	How to Exercise	Timeline
Access	Get a copy of data (including rewards)	In-app export or email support@guardianai.info	30 days
Rectification	Correct inaccurate data	In-app edit or email support@guardianai.info	Immediate/14 days
Erasure	Delete account and data (forfeit rewards)	In-app delete or email support@guardianai.info	30 days (90 for backups)

Object	Stop certain processing (may lose rewards)	Email support@guardianai.info with details	14 days assessment
Restrict	Pause processing	Email support@guardianai.info with reason	Immediate upon request
Portability	Export in machine-readable form	In-app export or email support@guardianai.info	14 days
Withdraw Consent	Revoke location/marketing/sharing/rewards	Device/App settings or email support@guardianai.info	Immediate effect
Lodge Complaint	File with regulator	TDRA/DIFC/ADGM as applicable	Varies by authority
Human Review	Contest automated decisions	In-app dispute or email support@guardianai.info	14 days review
Human Review (Rewards)	**Contest automated rewards decisions**	**Rewards tab > Dispute or email support@guardianai.info (subject: "Rewards Appeal")**	**21 days review**

End of Privacy Notice

Version: 1.1
Last Updated: November 6, 2025
Effective Date: November 6, 2025