

**HULLCORE · PRIVACY**

Privacy Policy

How the Hullcore flagship application handles personal data, under Turkish Law No. 6698 (KVKK) and, where applicable, GDPR. Publisher: Osman Can Çınar. Contact: legal@hullcore.dev. The binding language is Turkish — see the Turkish page for the authoritative text.

1. Introduction & Scope

This Privacy Policy explains how Hullcore (Osman Can Çınar) ("we") processes your personal data through the Hullcore application (mobile and web) and its backend services, in accordance with the Law on the Protection of Personal Data No. 6698 ("LPPD") and, where applicable, the EU General Data Protection Regulation ("GDPR"). It forms an integral part of the Terms of Use.

Account model

You may use map/browse/search features without an account; no personal data is requested in guest mode.

To use all features you register with an e-mail address and password. During registration the KVKK notice and this Policy are presented, and optional marketing consent may be granted.

2. Personal Data We Collect

Data category	Data	When	Purpose basis
Identity Data	Full Name (optional)	collected	LPPD Art. 5/2-c (necessary for a contract)
Contact Data	E-mail Address	collected	LPPD Art. 5/2-c (necessary for a contract)

Data category	Data	When	Purpose basis
Transaction Security Data	IP Address, User Account Information, Password (stored as a hash), Session/authentication tokens (and, if enabled, secure session + CSRF cookies), Device Information, Security and authentication log records, Push notification device token (FCM), Access-audit and security-event log records (which sensitive fields were read, by whom, when; login/lockout/2FA/role-change events)	collected	LPPD Art. 5/2-c, 5/2-c, 5/2-e, 5/2-f (contract; legal obligation; establishment of a right; legitimate interest); LPPD Art. 5/1 (explicit consent)
Identity/Contact Data (Apple)	Apple account identifier and verified/relay e-mail (from the Apple ID token)	only when you use / enable it	LPPD Art. 5/2-c (necessary for a contract)
Marketing Data	Notification preferences, commercial-communication consent status	only when you use / enable it	LPPD Art. 5/1 (explicit consent)
Visual and Audio Data	Photo / image (camera or photo-library content, user-initiated)	only when you use / enable it	LPPD Art. 5/2-c (necessary for a contract)
Location Data	Location (GPS) information, only when a location-based feature is used	only when you use / enable it	LPPD Art. 5/2-c (necessary for a contract)
Transaction Security / Usage Data	Diagnostics/crash data and product-usage events	only when you use / enable it	LPPD Art. 5/1 (explicit consent)

We do not collect data beyond what is listed above. In particular we do not collect advertising identifiers (AD_ID/IDFA), the content of your messages or calls, your web-browsing history, or device hardware identifiers (IMEI/MAC/serial), and we use no third-party advertising network. The Analytics/Crashlytics SDK initializes on every launch, but collection itself stays off until you opt in; when enabled, analytics providers receive no user identity, hardware identifiers, or advertising identifiers, and performance data is aggregated rather than per-user. Functional and transactional messages (security, account, and service notices) are independent of marketing consent and may always be sent. The mobile app uses encrypted local storage rather than cookies; any web surface

uses only essential cookies by default, and analytics or marketing cookies are set solely with your consent (Consent Mode v2, default off).

3. Consent Model (all optional consents off by default)

The following are processed only with your explicit consent and can be withdrawn at any time from Settings:

- Optional analytics / diagnostics
- Marketing / commercial communications

4. Purposes & Legal Basis

We process your data under LPPD Art. 5 / GDPR Art. 6 for:

- 2. Conducting Information Security Processes
- 8. Conducting Audit / Ethics Activities
- 10. Managing Access Authorizations
- 11. Ensuring Activities Comply with Legislation
- 16. Pursuing and Conducting Legal Matters
- 18. Conducting Communication Activities
- 20. Conducting Business Activities
- 46. Ensuring Security of Data Controller Operations
- 50. Providing Information to Authorized Persons, Institutions, and Organizations

And, subject to your explicit consent (LPPD Art. 5/1 / GDPR Art. 6(1)(a)):

- 21. Receiving and Evaluating Suggestions for Improving Business Processes
- 22. Conducting Business Continuity Activities
- 45. Conducting Product / Service Marketing Processes

5. Third-Party Service Providers & Cross-Border Transfer

In the current Hullcore demo build, no external service provider is enabled by default; all provider seams run in a built-in no-op mode. The template below lists the providers a



deployment may enable.

Where personal data is transferred abroad, we rely on a Board-registered Standard Contract with five-business-day notification to the Personal Data Protection Board (LPPD Art. 9), or on Standard Contractual Clauses or an adequacy decision under GDPR Chapter V; data-processing agreements bind every processor to instruction-only processing.

6. Data Security

We protect data with TLS 1.2+ and certificate pinning in transit; AES-256-GCM at rest on the backend, field-level PII encryption on iOS and SQLCipher on Android; the production backend refuses to start without a real encryption key; role-based access controls and full audit logging.

7. Retention

We retain each category of personal data for the period stated below. Where legislation prescribes a period (e.g. financial records), that statutory period governs; otherwise data is kept only as long as needed for the processing purpose. On expiry it is deleted, destroyed, or anonymized (LPPD Art. 7).

Data category	Retention period
Identity Data	Until account deletion, then a 30-day backup purge
Contact Data	Until account deletion, then a 30-day backup purge
Transaction Security Data	Session/authentication tokens: token lifetime only. Account and security records (password hash, device info, consent-proof IP/User-Agent): until account deletion + 30-day backup purge; Push token: until logout or token invalidation; 1 year (security and legal-consent audit records)
Identity/Contact Data (Apple)	Until account deletion, then a 30-day backup purge
Marketing Data	Until consent is withdrawn / unsubscribe
Visual and Audio Data	Until account deletion; user-deletable at any time
Location Data	Transient use (navigation/nearby): not stored. Where the app persists location (history/tracking/geofence): until account deletion, user-deletable at any time

Data category	Retention period
Transaction Security / Usage Data	14 months, and only if analytics is enabled (off by default)

8. Deletion & Account Closure

You may delete your account at any time from within the app; on deletion your data is removed from the device and backend, and backups are purged on a 30-day cycle. If you withdraw consent or ask us to delete your data, we destroy it without waiting for the periodic-destruction cycle (KVKK m.7). Records subject to a statutory period — commercial/financial records (10 years, Turkish Commercial Code m.82) and tax documents (5 years, Tax Procedure Law m.253) — are kept in a restricted archive used solely to meet that obligation and destroyed at its end. We do not keep a general litigation archive of account data.

9. Your Rights

Under LPPD Art. 11 (and, where applicable, GDPR Art. 13–22) you may learn whether your data is processed, request information, correction, deletion, or object to processing, and request data portability. You exercise these rights by applying to the data controller under LPPD Art. 13 and the Communiqué on Application Procedures (10.03.2018): via the Data Subject Application Form at <https://hullcore.dev/kvkk/data-subject-request-form>, by e-mail to legal@hullcore.dev; anyone applying on your behalf must present a notarized power of attorney. We conclude your application within thirty days at the latest, free of charge (a fee under the Board's tariff may apply where the process requires additional cost). If you are dissatisfied with the response, you may complain to the Personal Data Protection Board under LPPD Art. 14 within thirty days of learning the response and in any event within sixty days of your application.

10. Device Permissions

The app requests the following permissions just-in-time, only when a feature that needs them is used:

- Photos / Camera

- Camera
- Location

II. Age, Changes & Contact

The app is intended for users aged 18 and over; if we learn that we have processed a minor's data, we delete it without undue delay. We may update this Policy; material changes are notified in-app and/or by e-mail and take effect after the stated notice period. Contact: legal@hullcore.dev · <https://hullcore.dev>.

Hullcore (Osman Can Çınar) · legal@hullcore.dev · <https://hullcore.dev> Version 1.0 · effective on publication Prepared in compliance with Google Play Developer Policies, Apple App Store Review Guidelines, LPPD, and GDPR.



Hullcore

License the foundation. Ship your product.

A product built by Osman Can Çınar



✉ info@hullcore.dev ✉ legal@hullcore.dev ✉ can.cinar@hullcore.dev

© 2026 Osman Can Çınar. Hullcore™ is a trademark of Osman Can Çınar. · hullcore.dev

[Privacy Policy](#) · [Terms of Use](#) · [EULA](#) · [KVKK Notice](#) · [KVKK Application Form](#) · [Sub-processors](#) · [Data Deletion](#)