Privacy Policy

Effective Date: 2025-09-01

This Privacy Policy explains how **Kronos LLC** (“Company”, “we”, “us”, “our”) collects, uses, discloses, and protects information when you use our mobile applications and the website **the-kronos.com** (collectively, the “Services”).

Legal Entity: Kronos LLC
Email for privacy requests: info@the-kronos.com
Website: https://the-kronos.com

---

1. What Data We Process

1.1. Identifiers (Tracking)

- Device ID, User ID, advertising identifiers IDFA/GAID (for ads/attribution, with consent where required).
- On iOS we comply with App Tracking Transparency (ATT) and display the system consent prompt when tracking applies.

1.2. Data Linked to You

- Identifiers: User ID, Device ID.
- Purchases: transaction/subscription status, productId, subscription type.

1.3. Data Not Linked to You

- Usage Data: interactions, events, ad impressions/clicks.
- Diagnostics: crash reports, performance, technical telemetry.
- Contact Info: e-mail (only when you provide it for support or feedback).

1.4. In-App Purchases (IAP) & Payments

- App Store / Google Play provide order/receipt identifiers, productId, purchase time/status, and store country.
- We do not receive card/bank details.
- Receipts/tokens may be stored as needed to verify purchases, prevent fraud, and restore access.

1.5. Push Notifications

- FCM/APNs tokens to deliver notifications.
- Message content is minimal (service updates; marketing messages only with your consent).

1.6. Remote Configuration & Experiments

- Unity Remote Config / Firebase Remote Config may use technical identifiers and usage events to run A/B tests and adapt UI/features.

1.7. Security Logs

- IP address, device/OS info, timestamps, and technical events for security, abuse prevention, and support.

---

2. Sources & Permissions

2.1. Data Sources

- Information you provide directly (e-mail, support forms, in-app requests).
- Automatically collected technical data while using the Services.
- Third-party providers: Google Ads/AdMob, Firebase (Analytics/Crashlytics/Cloud Messaging), Unity (Ads/Analytics/UGS/Remote Config), payment platforms, app stores, ad networks — within your device permissions.

2.2. Device Permissions (OS-Level)

- Notifications (Push) for service messages.
- Advertising ID — IDFA/GAID (you can revoke/limit it in OS settings).
- Location / Camera / Microphone / Photos / Files — only if needed for specific features; we show the system prompt and explain the purpose.
- Game Center / Google Play Games for achievements/leaderboards (if available).

2.3. Cookies & Similar Technologies (Website)

On the-kronos.com we may use cookies, local storage, and third-party pixels for:

- strictly necessary site functions;
- analytics (e.g., Google Analytics/Firebase);
- marketing/retargeting — with your consent.

Manage preferences via the consent banner or your browser settings.

---

3. Legal Bases & Roles

- Contract performance (operate the Services).
- Consent (personalized ads/ATT/marketing emails).
- Legitimate interests (security, fraud prevention, aggregated analytics).
- Legal obligations (accounting, compliance).

3.1. Who Does What

Kronos LLC is the data controller for most processing. Vendors (Google, Unity, etc.) act as processors or joint controllers (per their terms). We enter into DPAs and implement appropriate safeguards.

---

4. How We Use Information

- Provide and maintain the Services.
- Process purchases/subscriptions and grant access (IAP: StoreKit / Google Play Billing; receipt verification).
- Analyze usage and stability (Firebase/Unity Analytics; Crashlytics/Cloud Diagnostics).
- Run A/B tests and remote configuration (Unity/Firebase Remote Config).
- Serve ads (non-personalized or personalized only with consent) via Google Ads/AdMob and Unity Ads.
- Communicate with you (support, important notices, newsletters with consent) and send push notifications.
- Protect rights, prevent abuse, and ensure security.

---

5. Sharing with Third Parties

We share data only as necessary:

- Service providers: analytics, hosting, crash reporting, e-mail, app stores/payments.
- Advertising partners: only with your consent and according to your privacy settings.
- Authorities: when required by law or to protect rights/safety.

We do not sell personal data.

5.1. Key Vendors

- Google — Ads/AdMob; Firebase Analytics; Firebase Crashlytics; Firebase Cloud Messaging.
- Unity — Unity Ads; Unity Analytics; Unity Gaming Services (Remote Config, Cloud Diagnostics).
- App Stores — Apple StoreKit and Google Play Billing for payments/verification.

- Communications/Support — e-mail providers/helpdesk tools.

- Others as needed — hosting/CDN, A/B testing, anti-fraud.

---

6. Your Choices & Controls

- iOS: Settings → Privacy & Security → Tracking (revoke tracking consent).

- Android: Google Settings → Ads → Delete advertising ID / Opt-out of Ads Personalization.

- In-app (where available) you can disable personalized ads (Google/Unity) — we will serve contextual/non-personalized ads.

- Push notifications can be turned off in system settings or in-app.

- Do Not Track (DNT) is not standardized; we provide the controls above instead.

- Unsubscribe from marketing e-mails via the unsubscribe link or by contacting us.

---

7. Data Retention

Typical periods (may vary by product/law):

- IAP receipts/tokens — up to 24 months.

- Crash logs/diagnostics — up to 90 days.

- Analytics events — up to 24 months, then aggregated/anonymous.

- FCM/APNs tokens — while push is active or until user deletion.

- Account/identifiers — while access is active or needed to provide the Services.

After these periods we delete or de-identify data unless required otherwise by law.

---

8. Security

We implement technical and organizational measures: encryption in transit, access controls, logging, and regular reviews.

8.1. Incident Response

In case of a personal data breach we will:

- assess risks and scope;
- notify EEA supervisory authorities within 72 hours where required;
- inform affected users if there is a high risk.

---

9. Your Rights

You may have rights to access, rectify, erase, restrict/object to processing, data portability, and withdraw consent.

How to submit a request: e-mail **info@the-kronos.com** with subject *Privacy Request*, specify the right you wish to exercise and your user/device identifier. We may ask for identity verification. We respond within statutory timeframes.

- **EEA/UK**: you may lodge a complaint with your local data protection authority.
- **California (CCPA/CPRA)**: rights to know/delete/limit use of sensitive data. We do not “sell” personal information as defined by CCPA and do not “share” it for cross-context behavioral advertising without your consent.

---

10. International Transfers

Data may be processed outside your country. We use appropriate safeguards (e.g., EU Standard Contractual Clauses). Vendors (Google, Unity, etc.) may store data in multiple regions.

---

11. Children’s Privacy

The Services are not directed to children under 13 (or higher age as required by local law). We do not knowingly collect data from children. If you believe a child provided data to us, contact us and we will delete it.

---

12. Changes to This Policy

We may update this Policy from time to time. The current version will always be available in the apps and/or on our website. For material changes, we will provide notice through the Services or by other appropriate means.

---

13. Contact

Kronos LLC

E-mail: info@the-kronos.com

Website: https://the-kronos.com

Appendices

Appendix A — Data Category Map (Apple Privacy Labels)

- Identifiers (Tracking): Device ID, User ID, IDFA/GAID — ads, attribution, analytics — while account is active.

- Identifiers (Linked): User ID, Device ID — core functionality, security, support — while access is active.

- Purchases: transactions/subscriptions — content access, accounting — statutory accounting periods.

- Usage Data: interactions, ad events — analytics, improvements — aggregated longer, raw logs shorter.

- Diagnostics: crash/performance — diagnostics, security — up to 90 days (aggregated longer).

- Contact Info: e-mail — support/communications — while case is active or until consent is withdrawn.

Appendix B — Vendor Policies

- Google / AdMob / Ads: https://policies.google.com/privacy

- Firebase: https://firebase.google.com/support/privacy

- Unity: https://unity.com/legal/privacy-policy

- Apple: https://www.apple.com/legal/privacy/

Appendix C — Opt-Out & Controls

- iOS: Settings → Privacy & Security → Tracking.

- Android: Google Settings → Ads → Delete advertising ID / Opt-out of Ads Personalization.

- In-app (where available): disable personalized ads/analytics.

- Push: disable in system settings or in-app.

Appendix D — Data Subject Request Template

Subject: Data Request — [type of request]
I am a user of [app name] and request [access/export/deletion] of my personal data.
User ID (if known):__.
I confirm ownership of the account and am ready to verify my identity.
Date / Signature.