

PRIVACY POLICY

Booster Gaming Mode Lower Lag

Package: com.quantumcore.gamemodeelite

Effective Date: June 20, 2026 **Last Updated:** June 20, 2026

Version 2.0

1. Introduction

This Privacy Policy (the “**Policy**”) describes how **Booster Gaming Mode Lower Lag** (also referred to as the “**Application**,” the “**App**,” “**we**,” “**us**,” or “**our**”) collects, uses, processes, stores, discloses, and protects information when you install, access, or use our Android mobile application distributed through the Google Play Store under the package name **com.quantumcore.gamemodeelite**.

Booster Gaming Mode Lower Lag is a performance optimization utility designed to enhance the gaming experience on Android devices by providing real-time performance monitoring, network optimization, thermal management, notification control, and related features. We are committed to safeguarding the privacy of our users and to complying with applicable data protection laws, including the European Union General Data Protection Regulation (GDPR), the United Kingdom Data Protection Act 2018, the California Consumer Privacy Act and California Privacy Rights Act (CCPA/CPRA), the Brazilian General Data Protection Law (LGPD), and the Google Play Developer Program Policies, including the Data Safety requirements.

By downloading, installing, or using the Application, you acknowledge that you have read, understood, and agreed to the practices described in this Policy. If you do not agree with any provision of this Policy, please refrain from installing or using the Application.

This Policy applies exclusively to the Application and does not extend to any third-party websites, applications, or services that may be linked to, integrated with, or accessed through the Application. Each third-party service maintains its own privacy practices, and we encourage you to review their respective privacy policies.

2. Definitions

For the purposes of this Policy, the following terms shall have the meanings set forth below:

- “**Personal Data**” or “**Personal Information**” means any information relating to an identified or identifiable natural person, as defined under applicable data protection laws.
- “**Processing**” means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination, restriction, erasure, or destruction.
- “**Data Controller**” refers to the entity that determines the purposes and means of processing Personal Data.
- “**Data Processor**” refers to the entity that processes Personal Data on behalf of the Data Controller.
- “**User**,” “**you**,” or “**your**” refers to the individual installing, accessing, or using the Application.
- “**Device**” means the Android smartphone, tablet, or other mobile device used to access the Application.

- **“Anonymous User Identifier”** means a randomly generated identifier (UUID) created by Supabase Anonymous Authentication, which is not linked to any directly identifying information such as your real name, email address, or phone number.
- **“Subscription”** means any paid subscription tier offered through the Application and processed through Google Play Billing and RevenueCat.

3. Data Controller and Contact Information

The data controller responsible for the processing of your information through the Application is:

DevNexa LLC

Operating the Application: **Booster Gaming Mode Lower Lag**

Contact Email: admin@devnexalabs.com

Postal Address:

30 N Gould St Ste R, Sheridan, WY 82801, United States

For any privacy-related inquiries, requests, or concerns, please contact us using the details provided in Section 17 (Contact Information).

4. Information We Collect

The Application is designed with a privacy-first approach. We collect only the information necessary to deliver and improve our services, to operate subscriptions, and to comply with legal obligations. The categories of information we collect are described below.

4.1 Information You Provide Directly

The Application does not require you to create a traditional account or to provide directly identifying information such as your real name, email address, phone number, postal address, or government-issued identifiers. The Application uses Supabase Anonymous Authentication, meaning that you may use the App without revealing your identity.

If you contact us for support, you may voluntarily provide contact information (such as an email address) so that we can respond to your inquiry. We will use that information solely for the purpose of responding to your request and resolving the matter.

4.2 Information Collected Automatically

When you install and use the Application, the following categories of information may be collected automatically:

4.2.1 Authentication and Device Identifiers

- **Anonymous User Identifier (UUID):** Upon first launch, the Application authenticates you through Supabase Anonymous Sign-In. This generates a unique, randomly produced UUID that is

associated with your installation. The UUID does not contain or reveal any directly identifying information.

- **Device Identifier:** A device identifier derived from the Android Secure Settings `ANDROID_ID` (with a randomly generated UUID stored in local preferences as a fallback) is used to distinguish your specific device installation, enabling features such as multi-device support and session continuity.

4.2.2 Device and Hardware Information

To provide accurate performance optimization recommendations, the Application collects the following technical information about your device:

- Device manufacturer (e.g., Samsung, Xiaomi, Huawei)
- Device model and model number
- Android SDK level and Android operating system version
- Total device RAM (in megabytes)
- Number of CPU cores available
- Display screen refresh rate and supported refresh rates
- Whether the device has a display notch or cutout
- Application version installed
- Device language and locale settings

4.2.3 Real-Time Performance Metrics

During active boost sessions, the Application reads system-level performance metrics to display them in real time and to provide post-session reports. These metrics include:

- Available and total RAM (read from `ActivityManager.MemoryInfo`)
- CPU usage percentage (read from `/proc/self/stat` for the Application process only)
- Frames per second (FPS) measured via the Android Choreographer API
- Battery temperature in Celsius (read from `BatteryManager`)
- Battery charge level and charging status
- Network ping (measured via TCP socket connections to public endpoints on port 443, including Cloudflare 1.1.1.1; see Section 8.5)
- Network jitter and packet loss indicators
- Network download and upload speed estimates (via Android `TrafficStats`)

4.2.4 Session Data

When you initiate a boost session, the following session-related information is recorded and may be transmitted to our backend for reporting purposes:

- Session start time and end time
- Session duration in milliseconds
- Type of boost (manual, automatic, or competitive)

- The game package name associated with the session, if a registered game is detected in the foreground
- Aggregated performance metrics (e.g., average FPS, average ping, maximum temperature, RAM freed)
- Number of stutter events detected and their severity
- Number of notifications blocked during the session
- A calculated session score (zero to five stars) based on overall performance

4.2.5 Game Library Information

When you add a game to your library, or when the Application detects an installed game on your device, the following information is stored:

- Game package name (e.g., com.tencent.ig)
- Application display name
- Whether the game is marked as online or heavy
- Custom per-game settings such as preferred FPS profile, brightness level, volume level, and orientation
- Total play time and last-played timestamp

4.2.6 Foreground Application Detection (Usage Access)

With your express consent (granted through the Android system Usage Access settings), the Application periodically queries the most recently foregrounded application package via Android's UsageStatsManager. The Application uses this information solely to determine whether a registered game is currently in the foreground, in order to enable the Auto Game Detection and automatic boost features. The Application does not collect, retain, or transmit broad usage history; only the matched game package name is persisted as part of session data.

4.2.7 Network Server Performance Data

When you initiate a ping test against game servers or public network endpoints, the Application records:

- The server tested (game name, server name, region)
- The measured ping in milliseconds
- The timestamp of the test
- Which server was identified as the fastest

4.2.8 Subscription and Purchase Information

If you purchase a subscription through the Application, the following information is processed by our backend and by RevenueCat:

- Subscription status (free, trial, active, expired, grace period, cancelled)
- Product identifier of the purchased subscription
- Subscription start date, expiration date, and trial end date (where applicable)

- RevenueCat customer identifier (which equals your Anonymous User Identifier)
- Transaction identifiers
- Whether the subscription is in grace period or auto-renewing
- The environment of the transaction (sandbox or production)

Important: we do not collect, process, or store your payment card details, banking information, or Google account credentials. All payment processing occurs entirely within Google Play's secure billing system. We receive only the purchase metadata necessary to validate and manage your subscription.

4.2.9 Diagnostic and Crash Data

Through Firebase Crashlytics, we automatically collect technical diagnostic information whenever the Application encounters an error or crash, including:

- Stack traces and error logs
- Application version and build identifier
- Android operating system version
- Device model and hardware identifiers
- Timestamp and state of the Application at the time of the crash
- A Crashlytics installation identifier (UUID) automatically generated by the Firebase Crashlytics SDK

4.2.10 Analytics Data

Through Firebase Analytics, we collect aggregated and pseudonymized data regarding how users interact with the Application, including:

- App launch events and session counts
- Screen views and feature interactions
- Subscription conversion events
- Geographic region (derived from IP address, used primarily in aggregate form)
- Device category and Android version distribution
- App instance identifier automatically assigned by the Firebase Analytics SDK

4.2.11 Advertising Identifier (Google Advertising ID)

Important disclosure. Because the Application integrates the Firebase Analytics SDK, the Google Play Services library may automatically collect your device's **Google Advertising ID (AAID/AD_ID)**. The Advertising ID is a resettable identifier provided by Google Play Services and is used by Firebase Analytics for analytics, attribution, and conversion measurement. We do not use the Advertising ID for personalized advertising, and we do not share it with advertising networks for ad targeting purposes. You may reset your Advertising ID, or opt out of personalized advertising, at any time through your device's *Settings > Privacy > Ads* menu.

4.2.12 Push Notification Tokens

Through Firebase Cloud Messaging (FCM), the Application is assigned a unique FCM registration token. This token allows us to deliver push notifications related to subscription status, important service announcements, app updates, and (with your consent) optional promotional content. The token is associated with your device installation and may be stored alongside your Anonymous User Identifier in our backend.

4.2.13 Internet Protocol (IP) Address

Whenever the Application communicates with our backend (Supabase), with RevenueCat servers, with Firebase services, or with the public ping endpoint operated by Cloudflare, the receiving servers observe the IP address from which the request originates. We do not store raw IP addresses in our application database. Our third-party processors (Supabase, RevenueCat, Google/Firebase, and Cloudflare) may temporarily log IP addresses for security, abuse-prevention, and operational diagnostic purposes in accordance with their respective privacy policies.

4.3 Information We Do Not Collect

For the avoidance of doubt, we explicitly do not collect the following categories of information:

- Your real name, date of birth, or government identification
- Your email address (unless you voluntarily contact us)
- Your phone number or contact list
- Your precise geographic location (GPS coordinates) or coarse location
- The contents of your text messages, emails, or any private communications
- Photos, videos, or audio recordings stored on your device
- Files or documents outside of the Application's own cache directory
- Browsing history from your web browser or any other application
- Payment card details, banking credentials, or Google account passwords
- Biometric data such as fingerprints or facial recognition data
- Health, fitness, or medical information

Accessibility Services. The Application does **not** register or operate any Android AccessibilityService. The Application does not read on-screen content, intercept input events, or use the BIND_ACCESSIBILITY_SERVICE permission.

5. Permissions Used by the Application

The Application requests the following Android permissions. Each permission is requested only when necessary for a specific feature, and we explain the purpose of each permission before requesting it (a model known as Smart Permission Requests). You may revoke any permission at any time through your device's system settings.

5.1 INTERNET

Required to communicate with our backend services (Supabase), Firebase services, and RevenueCat servers, and to perform network optimization features such as ping measurement and connection testing.

5.2 ACCESS_NETWORK_STATE

Used to detect whether the device is connected to a network and to identify the type of connection (Wi-Fi or mobile data). This permission is also a standard runtime requirement of certain integrated SDKs (Firebase, OkHttp, Ktor).

5.3 FOREGROUND_SERVICE and FOREGROUND_SERVICE_SPECIAL_USE

Required to run the Boost Service and the Game Monitor Service as foreground services with the “specialUse” subtype. The Boost Service maintains an ongoing notification that displays the session timer and provides quick controls during an active gaming session. The Game Monitor Service is used solely to detect when a registered game enters the foreground in order to trigger the Auto Boost feature. Each foreground service declares an Android FGS-subtype property describing its purpose (game_performance_boost_session and game_launch_detection respectively).

5.4 POST_NOTIFICATIONS (Android 13 and above)

Required to display the persistent session notification, alerts related to subscription status, push notifications delivered through Firebase Cloud Messaging, and other service-related notifications. The Application gracefully handles the absence of this permission.

5.5 SYSTEM_ALERT_WINDOW (Display Over Other Apps)

Required to display the optional Heads-Up Display (HUD) overlay and the Ping Overlay above other applications, including games. These overlays show real-time performance metrics such as FPS, ping, RAM, CPU usage, and temperature. The Application requests this permission only when you explicitly attempt to enable the HUD feature, and the permission can be revoked at any time through your device settings.

5.6 ACCESS_NOTIFICATION_POLICY

Required to enable the Do Not Disturb (DND) Mode during gaming sessions. When activated, this allows the Application to silence non-essential notifications and sounds while you are playing. This permission is requested only when you explicitly enable DND functionality, and we display a detailed explanation before initiating the request.

5.7 PACKAGE_USAGE_STATS (Usage Access)

Required to detect which application is currently in the foreground, enabling the Auto Game Detection feature. The Application reads the package name of the currently active app to determine whether it matches a registered game in your library. No detailed usage history is collected or transmitted; only the matched game package name is processed and stored as part of session data.

5.8 REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

Requested optionally to allow the Boost Service to continue running without interruption during long gaming sessions, particularly on devices from manufacturers (such as Xiaomi, Huawei, Oppo, OnePlus,

Vivo, and Samsung) that implement aggressive battery optimization. The Application is functional without this permission, although session interruptions may occur on certain devices.

5.9 RECEIVE_BOOT_COMPLETED

Used optionally to start a lightweight monitoring service when your device boots, allowing the Auto Boost feature to detect game launches automatically. No heavy operations are performed at boot time, and this feature can be disabled at any time.

5.10 VIBRATE

Used to provide haptic feedback during boost actions, button presses, and other interactive elements.

5.11 BILLING (com.android.vending.BILLING)

Required to process subscription purchases through Google Play Billing. This permission allows the Application to communicate with the Google Play Store in order to manage in-app subscriptions, restore previous purchases, and verify subscription status.

5.12 Detection of Installed Games (Scoped Package Visibility)

The Application does **not** declare the QUERY_ALL_PACKAGES permission. Instead, the Application uses Android's scoped *<queries>* manifest element to declare a limited and explicit set of game package names that it is permitted to detect, together with a query for applications that respond to the standard MAIN/LAUNCHER intent. This approach limits app-inventory visibility to that which is strictly necessary to populate the in-app Game Library. No information about non-game applications is transmitted to our servers.

5.13 Automatically Merged Permissions from Integrated SDKs

Certain permissions are automatically merged into the Application's manifest by the build system as required by the Firebase SDKs we integrate. These include, without limitation:

- **com.google.android.gms.permission.AD_ID** – merged by the Firebase Analytics library; enables access to the Google Advertising ID for analytics measurement (see Section 4.2.11).
- **com.google.android.c2dm.permission.RECEIVE** and related internal permissions – merged by Firebase Cloud Messaging to enable the receipt of push notifications.

6. How We Use Your Information

We use the information collected through the Application for the following purposes:

- **Service Provision:** to deliver the core functionality of the Application, including performance monitoring, network optimization, thermal management, game detection, and session reporting.
- **Personalization:** to remember your preferences, settings, registered games, custom touch profiles, language selection, and feature toggles.
- **Subscription Management:** to verify your subscription status, deliver premium features, process renewals, and respond to billing inquiries.

- **Analytics and Improvement:** to understand how users interact with the Application, identify popular features, detect performance bottlenecks, and improve the overall user experience.
- **Crash Reporting and Stability:** to detect, diagnose, and resolve technical issues, crashes, and errors, thereby improving the stability and reliability of the Application.
- **Push Notifications:** to deliver notifications regarding subscription status changes, important service announcements, app updates, security alerts, and (with your consent) promotional content.
- **Security and Fraud Prevention:** to detect, prevent, and respond to fraudulent activity, abuse, security incidents, and violations of our Terms and Conditions.
- **Legal Compliance:** to comply with applicable legal obligations, respond to lawful requests from competent authorities, and enforce our legal rights.
- **Aggregated Statistics:** to produce anonymized and aggregated statistics about Application usage, which may be used for research, reporting, and business decision-making.

7. Legal Bases for Processing (GDPR / UK GDPR)

If you are a resident of the European Economic Area, the United Kingdom, or Switzerland, the legal bases on which we rely for processing your Personal Data are as follows:

- **Contract Performance (Article 6(1)(b) GDPR):** processing necessary to provide the Application's services to you, including subscription management.
- **Legitimate Interests (Article 6(1)(f) GDPR):** processing necessary for our legitimate business interests, such as analytics, fraud prevention, security, and product improvement, provided that these interests are not overridden by your fundamental rights and freedoms.
- **Consent (Article 6(1)(a) GDPR):** processing based on your specific consent, such as the use of certain permissions (SYSTEM_ALERT_WINDOW, ACCESS_NOTIFICATION_POLICY, PACKAGE_USAGE_STATS) and the delivery of promotional push notifications.
- **Legal Obligation (Article 6(1)(c) GDPR):** processing necessary to comply with our legal obligations under applicable law.

8. Third-Party Services and Data Processors

To deliver the Application's services, we rely on the following third-party service providers. Each of these providers acts as an independent data processor or sub-processor with respect to the data they receive on our behalf. Where personal data is transferred to these providers, appropriate contractual safeguards are in place.

8.1 Supabase, Inc.

- **Purpose:** Backend database (PostgreSQL), Anonymous Authentication, real-time data synchronization, and Edge Function execution (including the RevenueCat webhook handler).

- **Data Shared:** Anonymous User Identifier, device identifier and device information, session data, game library entries, app settings, subscription events, performance statistics, FCM registration token, and other data described in Section 4.
- **Privacy Policy:** <https://supabase.com/privacy>

8.2 Google LLC – Firebase Services

We use the following Firebase services, each of which is governed by Google's Privacy Policy and the Firebase Data Processing and Security Terms.

8.2.1 Firebase Analytics

- **Purpose:** to analyze user behavior, feature engagement, and conversion metrics, primarily in aggregated form.
- **Data Shared:** App instance identifier, screen views, events, device model, Android version, app version, language, country (derived from IP), Google Advertising ID (see Section 4.2.11), and other standard analytics events.

8.2.2 Firebase Crashlytics

- **Purpose:** to detect and report application crashes and non-fatal errors for diagnostic purposes.
- **Data Shared:** Stack traces, exception data, device model, Android version, app version, log statements preceding the crash, and a Crashlytics installation UUID.

8.2.3 Firebase Cloud Messaging (FCM)

- **Purpose:** to deliver push notifications to your device.
- **Data Shared:** Device FCM registration token and the content of the notifications themselves.

8.2.4 Firebase Remote Config

- **Purpose:** the Application integrates the Firebase Remote Config SDK to allow remote tuning of feature parameters and to support staged rollouts. This SDK is currently dormant and is not used to make any user-impacting decisions at this time.
- **Data Shared:** App instance identifier and minimal device metadata required for SDK operation.

Firebase Privacy Policy: <https://policies.google.com/privacy>

8.3 RevenueCat, Inc.

- **Purpose:** to manage in-app subscriptions, validate purchases, deliver subscription events to our backend via webhooks, and provide hosted paywalls.
- **Data Shared:** Anonymous User Identifier (used as the RevenueCat app_user_id), purchase tokens, product identifiers, subscription status, transaction history, store country, and standard device metadata used by the RevenueCat SDK.
- **Privacy Policy:** <https://www.revenuecat.com/privacy>

8.4 Google Play Billing

- **Purpose:** to securely process subscription purchases, renewals, and refunds.
- **Data Shared:** Subscription purchase tokens, product identifiers, purchase timestamps, subscription state, and (managed entirely by Google) payment information.
- **Privacy Policy:** <https://policies.google.com/privacy>

8.5 Cloudflare, Inc. (Public DNS / 1.1.1.1)

- **Purpose:** the Application performs latency measurements by opening a TCP connection on port 443 to the Cloudflare public endpoint at 1.1.1.1. No payload data is transmitted; only the connection establishment timing is measured.
- **Data Shared:** Solely the connection metadata inherent to any TCP handshake (source IP address, destination IP and port, timing). No Personal Data of yours is intentionally transmitted.
- **Privacy Policy:** <https://www.cloudflare.com/privacypolicy/>

9. Local Storage on Your Device

In addition to cloud-based processing, the Application stores certain data locally on your device to ensure that core functionality remains available offline and to improve performance. The local storage mechanisms used include:

- **SharedPreferences:** used to cache feature toggle states, language settings, performance level preferences, HUD opacity, detection delay, onboarding completion flag, subscription status cache, FPS and ping values for the home-screen widget, the locally generated device identifier, and other lightweight key-value preferences.
- **Application Cache Directory:** used by the Application for temporary files. This cache may be cleared by you through the in-app Cache Cleaner feature or through your Android system settings.
- **Application Database (Room):** used to store offline copies of certain entities such as game library entries and session metadata, allowing the App to function without an active internet connection.

You may clear all local data at any time by uninstalling the Application, or by clearing the App's data through your device settings (*Settings > Apps > Booster Gaming Mode Lower Lag > Storage > Clear Data*).

10. Data Retention

We retain your Personal Data only for as long as necessary to fulfill the purposes for which it was collected, including any legal, regulatory, accounting, or reporting requirements. Detailed retention periods are described below.

10.1 Automatic Server-Side Deletion (90-Day Policy)

Our backend (Supabase) is configured with scheduled database maintenance jobs (implemented via PostgreSQL `pg_cron`) that automatically and permanently delete user-related telemetry from our active database after a retention window. Specifically:

- **Detailed session telemetry** (network statistics, stutter events, blocked notification records, battery readings, and per-session metrics) is automatically deleted after **ninety (90) days**.
- **Server ping results** are automatically deleted after **thirty (30) days**.
- **Cache-clean logs and boost logs** are automatically deleted after **ninety (90) days**.
- **Aggregated daily summaries** (non-identifying statistics) may be retained indefinitely for statistical and historical reporting.

10.2 Retention by Account State

- **Anonymous User Profile:** retained for as long as you continue to use the Application. You may request deletion at any time, as described in Section 13.
- **Subscription Events:** retained for the period legally required by applicable financial and tax regulations.

10.3 Retention by Third-Party Processors

Third-party service providers apply their own retention policies, which we cannot unilaterally override. To the best of our knowledge:

- **Firebase Crashlytics:** typically retains fatal crash data for approximately ninety (90) days, with longer retention for unresolved issues, in accordance with Firebase's retention policy.
- **Firebase Analytics:** retains event-level data for the period configured in our Firebase project settings, which by default is between two and fourteen months depending on the data type.
- **RevenueCat:** retains subscription and transaction records in accordance with its own privacy policy and applicable accounting obligations.

Please refer to the privacy policies of each third-party provider for their authoritative retention practices.

11. Data Security

We implement appropriate technical and organizational security measures to protect your information against unauthorized access, accidental loss, alteration, disclosure, or destruction. These measures include:

- Transport Layer Security (TLS / HTTPS) encryption for all data transmitted between the Application and our servers and third-party processors
- Row-Level Security (RLS) policies in our Supabase database, ensuring that authenticated users can access only data scoped to their own Anonymous User Identifier
- Authentication via secure anonymous tokens managed by Supabase
- Database-level triggers that prevent unauthorized modification of subscription status from the client side
- Authorization-header verification of incoming webhook events from RevenueCat
- Idempotent webhook processing to prevent duplicate event handling
- Industry-standard secrets management for backend service credentials

- Regular security reviews of third-party dependencies and SDK versions

Despite these safeguards, no method of transmission over the Internet or method of electronic storage is one hundred percent secure. While we strive to use commercially acceptable means to protect your information, we cannot guarantee absolute security. You are responsible for maintaining the security of the device on which the Application is installed.

12. Your Rights

Depending on your jurisdiction, you may have the following rights with respect to your Personal Data:

- **Right of Access:** the right to request confirmation of whether we process your Personal Data and to obtain a copy of such data.
- **Right to Rectification:** the right to request correction of any inaccurate or incomplete Personal Data.
- **Right to Erasure (“Right to be Forgotten”):** the right to request deletion of your Personal Data, subject to certain exceptions (e.g., legal obligations).
- **Right to Restriction of Processing:** the right to request that we restrict the processing of your Personal Data under certain circumstances.
- **Right to Data Portability:** the right to receive your Personal Data in a structured, commonly used, machine-readable format.
- **Right to Object:** the right to object to processing based on legitimate interests.
- **Right to Withdraw Consent:** where processing is based on consent, the right to withdraw consent at any time without affecting the lawfulness of processing carried out prior to withdrawal.
- **Right to Lodge a Complaint:** the right to lodge a complaint with a competent data protection supervisory authority.

To exercise any of these rights, please contact us using the information provided in Section 17. We will respond to your request within the timeframe required by applicable law (typically within thirty days).

13. Data Deletion Requests

Because the Application operates under an anonymous authentication model and does not require you to create an account with personally identifying credentials, you may control and request deletion of your data using one or more of the following methods:

13.1 Automatic Server-Side Deletion

As described in Section 10.1, the majority of user-related telemetry stored on our servers is automatically and permanently deleted after a retention window of ninety (90) days (or thirty (30) days for server-ping results) through scheduled database maintenance jobs.

13.2 Local Device Deletion

You may permanently remove all locally stored data at any time by uninstalling the Application from your device, or by clearing the Application's data through your device settings (*Settings > Apps > Booster Gaming Mode Lower Lag > Storage > Clear Data*).

13.3 Deletion Request by Email

You may submit a written deletion request at any time by contacting us at admin@devnexalabs.com. To assist us in locating your records, please include, where possible, your Anonymous User Identifier (UUID), which is available within the Application's Settings screen. Upon receipt of a valid deletion request, we will permanently delete your Personal Data from our active databases within thirty (30) days. Residual copies of your data may persist in encrypted backup systems for a limited additional period before being permanently overwritten in accordance with our backup retention schedule.

13.4 In-App Deletion Feature

Where and when made available in a future release of the Application, an in-app data deletion control will be exposed within the Settings screen to allow you to initiate a deletion request directly from your device.

14. Opt-Out Options

You have the following opt-out options:

- **Push Notifications:** you may disable push notifications at any time through your device's notification settings or by revoking the POST_NOTIFICATIONS permission.
- **Analytics and Advertising ID:** you may opt out of personalized advertising and reset your Google Advertising ID at any time through your device's *Settings > Privacy > Ads* menu. You may further limit Firebase Analytics collection through Google's app-personalization settings.
- **Crash Reporting:** crash reporting through Firebase Crashlytics may be disabled in your device's Google account settings where supported by your device manufacturer.
- **Optional Permissions:** all non-essential permissions (SYSTEM_ALERT_WINDOW, ACCESS_NOTIFICATION_POLICY, PACKAGE_USAGE_STATS, REQUEST_IGNORE_BATTERY_OPTIMIZATIONS) can be revoked at any time through your device's app-permission settings.
- **Subscription Management:** you may cancel your subscription at any time through the Google Play Store account-management settings.

15. International Data Transfers

Your information may be transferred to, and processed in, countries other than the country in which you reside. These countries may have data protection laws that are different from the laws of your country. Specifically, our third-party service providers (Supabase, Google/Firebase, RevenueCat, and Cloudflare) may store and process data in the United States, the European Union, and other jurisdictions.

Where required by applicable law, we ensure that appropriate safeguards are in place for international data transfers, such as the European Commission's Standard Contractual Clauses (SCCs), the UK International Data Transfer Addendum, or equivalent transfer mechanisms recognized under GDPR and UK GDPR.

16. Children's Privacy

The Application is not directed to, or intended for use by, children under the age of thirteen (13), or under sixteen (16) in jurisdictions where that is the minimum age for digital consent under applicable law (such as the European Economic Area). We do not knowingly collect Personal Data from children below the applicable minimum age.

If you are a parent or guardian and believe that your child has provided us with Personal Data, please contact us immediately. If we become aware that we have inadvertently collected Personal Data from a child below the applicable minimum age without verified parental consent, we will take steps to delete that information promptly.

17. Contact Information

If you have any questions, concerns, requests, or complaints regarding this Privacy Policy or our data practices, please contact us at:

Email: admin@devnexuslabs.com

Postal Address:

DevNexa LLC

30 N Gould St Ste R

Sheridan, WY 82801

United States

We aim to respond to all legitimate inquiries within thirty (30) days. For complex requests, additional time may be required, in which case we will notify you and keep you updated.

18. Google Play Compliance

This Application complies with the Google Play Developer Program Policies, including the User Data Policy, the Permissions and APIs Policy, the Subscriptions Policy, and the Data Safety requirements.

A detailed Data Safety declaration is published on the Application's Google Play Store listing, summarizing the categories of data collected, the purposes for which it is collected, whether the data is shared with third parties for their independent use, and whether the data is encrypted in transit and at rest. The Data Safety declaration is consistent with the disclosures made in this Privacy Policy.

If you have any concerns about our compliance with Google Play policies, you may contact us directly or report your concerns to Google through the Google Play Store.

19. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, the services we offer, or applicable legal requirements. When we make material changes, we will notify you by updating the “Last Updated” date at the top of this Privacy Policy and, where appropriate, by providing a more prominent notice within the Application (such as a push notification or an in-app banner).

We encourage you to review this Privacy Policy periodically. Your continued use of the Application after any changes constitutes your acceptance of the updated Privacy Policy.

20. Acknowledgement

By installing and using Booster Gaming Mode Lower Lag, you acknowledge that you have read and understood this Privacy Policy and consent to the collection, use, and disclosure of your information as described herein.

— End of Privacy Policy —