JORBI Privacy Policy and Clarification Text

Version: 1.0| Last Update: June 2026

Application Name: Jorbi ("Application" or "Platform")

Jorbi attaches the utmost importance to the privacy of its users and the protection of their personal data. By downloading or using the Application, you are deemed to have accepted this Privacy Policy. This policy has been prepared with the "Privacy by Design" principle, considering the KVKK (Turkey), GDPR (EU), and applicable international data protection regulations.

1. Data Controller and Contact Information

- **Data Controller (Name / Title):** Çiğdem Ertek Mutlu
- **Tax No:** 33154498546
- **Legal Notification Address:** Akarbaşı Mah. Ada Sk. Prestij Konutları C D Blok C Blok No: 33 İç Kapı No: 6 Odunpazarı / Eskişehir, Turkey
- **KVKK and Privacy Contact:** jorbiapp@gmail.com

2. Sensitive Data Declaration (Unprocessed Data)

Jorbi does not aim to process and does not request the provision of Special Categories of Personal Data (Sensitive Data) such as race, ethnic origin, political opinions, religious beliefs, clothing, association/foundation membership, health, sexual life, or biometric/genetic data.

3. Collected Data, Purposes of Processing, and Legal Basis (Matrix)

The minimum data collected due to the operation of the application, their purposes, and legal bases are transparently listed below:

Data Category	**Purpose of Processing**	**Legal Basis (KVKK / GDPR)**
Identity (Name, Surname, Username)	Account creation, in-platform social interaction.	Performance of a Contract
Contact (E-mail)	Account security, password reset, mandatory legal notifications.	Performance of a Contract / Legitimate Interest
Phone Number	Commercial account (Store)	Performance of a Contract / Legitimate

Data Category	Purpose of Processing	Legal Basis (KVKK / GDPR)
(Stores Only)	verification and OTP security.	Interest
Media (Camera and gallery)	Uploading profile photos and sharing post/event visuals.	Explicit Consent (Device Permission)
User Content (Posts, Comments)	Providing in-platform socialization and mutual interaction infrastructure.	Performance of a Contract
Messaging Data	Ensuring one-on-one secure communication between users.	Performance of a Contract
Location (Foreground GPS)	Displaying regional opportunities and store distance (150m) ticket approval.	Explicit Consent
Device ID (Hashed)	Preventing duplicate promotion abuse (Stores Only).	Legitimate Interest of the Data Controller
Network and Connection Data (IP Address)	Cyber security, logging obligations, preventing fake business registrations and abuse.	Legitimate Interest
Financial (Purchase Logs)	Defining the coin/token right (entitlement) to the account.	Performance of a Contract / Legal Obligation
Analytics and Crash Logs	Measuring application stability, fixing crash errors.	Legitimate Interest

Profile Enrichment Data: Information such as the city of residence, interests, and biography, provided entirely at the user's own request (optional), is processed under Explicit Consent to enrich the social structure.

Detailed Explanations on Data Processing Purposes:

- **Performance of the Contract:** Fulfilling the contractual obligations between the parties so that standard users (customers) can smoothly benefit from campaigns and opportunities on the platform; and commercial accounts (stores) can purchase tokens, create, plan, and publish campaigns.
- **Location-Based Verification:** Confirming the physical distance between the user and the store to prevent the abuse of opportunities.
- **Security and Prevention of Abuse:** Preventing fake location (Mock GPS) applications and protecting the commercial integrity of the platform. In this context, to prevent accounts previously restricted due to policy violations from infiltrating the platform again with different accounts using the same phone numbers or device IDs, security algorithms detecting policy-violating accounts and geofencing are operated.

4. Third-Party SDKs, Analytics, and Cookies

Jorbi does not engage in any advertising profiling (Ad Tracking) directed at users and does not sell your data to data brokers or advertising networks (e.g., Meta Ads, TikTok Ads). The SDK integrations implemented on the platform are:

- **Firebase Analytics:** Collects only anonymized usage statistics. Collected events are limited to application launch, screen viewing times, crash reports, and purchase flow success/error rates.
- **Firebase App Check / Crashlytics:** Your device model and operating system version are used to detect technical errors and prevent unauthorized access.

5. Notification and Announcement Infrastructure

- **Standard Users:** Our application uses the Push Notification infrastructure to instantly deliver new campaigns, squad invites, and friend requests to standard users (customers), and an anonymous notification token belonging to your device is processed for this purpose. You can turn off these notifications at any time from your device's operating system settings.
- **Store Accounts:** General informations and announcements made by the platform management to commercial accounts are not shown via the push notification infrastructure, but directly through the 'in-app message/announcement' panel within the store profile. These in-app announcements are part of the platform service and operate independently of the device's general notification permissions.

6. Profile Discoverability and Social Interaction

Posts and events shared by users are protected by default with high-level privacy and can only be viewed by people on the approved friends list. Third parties who are not on your friends list cannot directly access your personal content.

- **Discoverability:** Due to the social nature of the platform, your biography and friends list (who you are connected with) are visible on the platform to make it easier to establish new friendships.
- **Mutual Interactions:** When you comment on a post shared by a friend or participate in their event, these interactions can be seen by other mutual connections (even if you are not friends) who are authorized to see that content.

7. Messaging Privacy and Technical Security

One-on-one messaging contents are processed solely for the purpose of transmission between the parties. Message contents, by default, absolutely cannot be read or viewed by platform personnel or management. Security, spam, and abuse controls are conducted by the system through limited and automated metadata analysis, not by reading message contents.

8. Content Display Algorithm

The display of contents is algorithmically managed in two different areas:

- **Feed (Social):** Only the contents of approved friends are shown in chronological and interaction order.
- **Opportunities Page and Map:** Paid (tokenized) campaigns of businesses are ranked with a transparent algorithm based on the user's location, whether they follow the store, the priority of special campaign templates such as Flash Sale (20% and above discount), and a dynamic evaluation score based on the campaign's organic interaction rates (views, clicks, usage).

9. Content Moderation, Sanctions, and Appeal

To ensure a safe community environment, shared contents pass through a server-side dynamic profanity (swearing/insult) filter. In case of violation of the rules, the following sanctions are applied:

- **Temporary Suspension:** In case of a repeated violation, the account is restricted for a certain period.
- **Permanent Ban:** In case of detection of fraud, harassment, fake location (Mock GPS), or policy-violating behavior, the account is permanently deleted.
- **Appeal:** Users have the right to request a human review (SLA: 48 hours) regarding moderation decisions within 14 days via jorbiapp@gmail.com.

10. International Data Transfer

The Jorbi infrastructure predominantly runs on global service providers based in the US and the EU. In accordance with KVKK Article 9 and GDPR data transfer rules, considering the principle of data minimization, only the minimum data required by the relevant service is transferred to the following providers:

Service Provider (Country)	Transferred Data Category and Purpose of Use
Google Firebase / GCP (US / EU)	Authentication (Auth), user profiles, messages and posts (Firestore/Storage), analytical statistics, and crash logs.
Google Maps Platform (US / EU)	Only instant location (GPS) coordinates and regional campaign mapping data.
RevenueCat (US)	In-app purchase (ticket/token) logs and digital entitlement verification data (Card details are never transferred).
Apple App Store & Google Play (US)	Device security verification logs (App Attest / Play Integrity) and anonymous billing approvals.

All these transfers are carried out under the assurance of GDPR-compliant Standard Contractual Clauses (SCC) and ISO 27001 security certificates.

11. Legal Requests and Law Enforcement

Jorbi prioritizes user privacy. However, in the event of a proper, binding, and legal request from official authorities (Courts, Prosecutor's Offices, authorized Police units), the requested minimum data may be shared with the competent authorities to fulfill our legal obligations under applicable laws.

12. Data Retention Periods and Passive Accounts (TTL)

Pursuant to data minimization, automatic deletion (TTL) periods are as follows:

- **One-on-One Messages:** Permanently deleted after 90 days.
- **Notifications:** Automatically cleared after 30 days.
- **Short-Term Activities:** Removed from the system 2 hours after being shared.
- **Ticket and Session Logs:** Deleted after 48 hours for transaction security.
- **Campaign Data:** Campaigns that have expired or been closed by the store are permanently deleted from the database after 8 days in accordance with the data minimization principle.
- **Squad Data:** Successfully completed squad data is completely cleared from the system after 7 days, and incomplete (canceled) squad data after 3 days.
- **Human Interaction and Tagging:** When users tag stores (@store) in their posts, this content can be transferred to the store profile. The user is explicitly informed about

this situation with an in-app warning before sharing the post. To protect privacy, user names are masked (e.g., "jo..."). This data is not permanent on the store profile and is automatically cleared every morning at 08:00.
- **Passive Accounts:** Standard user accounts that have not been logged into continuously for 24 months and have fallen into an inactive (passive) state are permanently and automatically deleted from the system.

13. Account Deletion, Right to be Forgotten, and Data Portability

- **Account Deletion:** You can delete your account from the Settings > Delete My Account menu within the application or via the jorbi.app/delete-account address.
- **Standard Users:** When the deletion process is initiated, all personal data is instantly and permanently deleted.
- **Store Accounts:** To prevent repeated welcome token abuse, the e-mail, phone number, and device ID are stored by being one-way hashed using SHA-256. They are kept in locked security logs for 180 days. They are completely destroyed at the end of 180 days.
- **User Generated Content (UGC) License Duration:** In the event that the user deletes their account or removes the relevant content, the license and usage rights of these contents shall expire only at the end of a reasonable period required by technical backup processes.
- **Data Portability:** You can request a machine-readable copy of your data (in JSON or CSV format) via jorbiapp@gmail.com. Your request will be delivered within a maximum of 30 days.

14. Data Breach Procedure

Jorbi uses industry-standard encryption and firewalls to protect your data. In case any unauthorized access, cyber attack, or Data Breach is detected; affected users and competent data protection authorities (KVKK/GDPR DPA) will be informed transparently via e-mail within a maximum of 72 hours.

15. Child Safety and Age Limit

You must be at least 18 years old to use the Jorbi platform. During the registration phase, this condition is obtained with an age verification declaration. The platform does not knowingly collect data from children under the age of 18. If it is detected or reported that an account belongs to someone under the age of 18, the relevant account and all its data will be deleted immediately. Parents can report suspicious situations through our communication channel.

16. Policy Changes and Contact

Jorbi reserves the right to update this Privacy Policy. Significant changes will be announced via in-app notifications. For any applications and objections regarding your privacy, data portability, and KVKK/GDPR rights:

E-mail: jorbiapp@gmail.com