JORBI Datenschutzrichtlinie und Aufklärungstext

Version: 1.0 | Letzte Aktualisierung: Juni 2026

Anwendungsname: Jorbi („Anwendung“ oder „Plattform“)

Jorbi legt größten Wert auf die Privatsphäre seiner Nutzer und den Schutz ihrer personenbezogenen Daten. Durch das Herunterladen oder die Nutzung der Anwendung gelten diese Datenschutzrichtlinien als akzeptiert. Diese Richtlinie wurde unter dem Prinzip „Privacy by Design“ (Datenschutz durch Technikgestaltung) unter Berücksichtigung der KVKK (Türkei), der DSGVO (EU) und anwendbarer internationaler Datenschutzbestimmungen erstellt.

1. Verantwortlicher und Kontaktinformationen

- **Verantwortlicher (Name / Titel):** Çiğdem Ertek Mutlu
- **Steuer-Nr.:** 33154498546
- **Zustellungsadresse:** Akarbaşı Mah. Ada Sk. Prestij Konutları C D Blok C Blok No: 33 İç Kapı No: 6 Odunpazarı / Eskişehir, Türkei
- **KVKK und Datenschutz-Kontakt:** jorbiapp@gmail.com

2. Erklärung zu sensiblen Daten (Nicht verarbeitete Daten)

Jorbi zielt nicht darauf ab und fordert nicht die Bereitstellung besonderer Kategorien personenbezogener Daten (sensible Daten) wie Rasse, ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Kleidung, Vereins-/Stiftungsmitgliedschaften, Gesundheit, Sexualleben oder biometrische/genetische Daten.

3. Erhobene Daten, Verarbeitungszwecke und Rechtsgrundlage (Matrix)

Die aufgrund des Betriebs der Anwendung minimal erhobenen Daten, ihre Zwecke und Rechtsgrundlagen sind nachfolgend transparent aufgelistet:

Datenkategorie	**Verarbeitungszweck**	**Rechtsgrundlage (KVKK / DSGVO)**
Identität (Name, Nachname, Benutzername)	Kontoerstellung, soziale Interaktion innerhalb der Plattform.	Vertragserfüllung
Kontakt (E-Mail)	Kontosicherheit, Passwort-Zurücksetzung, obligatorische rechtliche Benachrichtigungen.	Vertragserfüllung / Berechtigtes Interesse

Datenkategorie	**Verarbeitungszweck**	**Rechtsgrundlage (KVKK / DSGVO)**
Telefonnummer (Nur Geschäfte)	Verifizierung des Geschäftskontos (Store) und OTP-Sicherheit.	Vertragserfüllung / Berechtigtes Interesse
Medien (Kamera und Galerie)	Hochladen von Profilfotos und Teilen von Beitrags-/Event-Bildern.	Ausdrückliche Einwilligung (Geräteberechtigung)
Nutzerinhalte (Beiträge, Kommentare)	Bereitstellung von plattforminterner Sozialisation und gegenseitiger Interaktionsinfrastruktur.	Vertragserfüllung
Nachrichtendaten	Gewährleistung einer sicheren Eins-zu-Eins-Kommunikation zwischen Nutzern.	Vertragserfüllung
Standort (Vordergrund-GPS)	Anzeige regionaler Angebote und Ticketgenehmigung nach Entfernung zum Geschäft (150m).	Ausdrückliche Einwilligung
Geräte-ID (Gehasht)	Verhinderung von Missbrauch durch doppelte Werbeaktionen (Nur Geschäfte).	Berechtigtes Interesse des Verantwortlichen
Netzwerk- und Verbindungsdaten (IP-Adresse)	Cybersicherheit, Protokollierungspflichten, Verhinderung falscher Geschäftsregistrierungen und Missbrauch.	Berechtigtes Interesse

Datenkategorie	Verarbeitungszweck	Rechtsgrundlage (KVKK / DSGVO)
Finanzen (Kaufprotokolle)	Zuweisung des Münz-/Token-Rechts (Entitlement) zum Konto.	Vertragserfüllung / Rechtliche Verpflichtung
Analysen und Absturzprotokolle	Messung der App-Stabilität, Behebung von Absturzfehlern.	Berechtigtes Interesse

Profilanreicherungsdaten: Informationen wie Wohnort, Interessen und Biografie, die der Nutzer völlig freiwillig (optional) angibt, werden mit Ausdrücklicher Einwilligung verarbeitet, um die soziale Struktur zu bereichern.

Detaillierte Erläuterungen zu den Datenverarbeitungszwecken:

- **Vertragserfüllung:** Erfüllung der vertraglichen Verpflichtungen zwischen den Parteien, damit Standardnutzer (Kunden) reibungslos von Kampagnen und Angeboten auf der Plattform profitieren können; und Geschäftskonten (Stores) Tokens kaufen sowie Kampagnen erstellen, planen und veröffentlichen können.
- **Standortbasierte Verifizierung:** Bestätigung der physischen Entfernung zwischen dem Nutzer und dem Geschäft, um den Missbrauch von Angeboten zu verhindern.
- **Sicherheit und Verhinderung von Missbrauch:** Verhinderung von Fake-Location-Apps (Mock GPS) und Schutz der kommerziellen Integrität der Plattform. In diesem Zusammenhang werden Sicherheitsalgorithmen und Geofencing eingesetzt, um zu verhindern, dass Konten, die zuvor wegen Richtlinienverstößen gesperrt wurden, mit denselben Telefonnummern oder Geräte-IDs unter anderen Konten wieder in die Plattform eindringen.

4. SDKs von Drittanbietern, Analysen und Cookies

Jorbi führt keine Werbeprofilerstellung (Ad Tracking) für Nutzer durch und verkauft Ihre Daten nicht an Datenbroker oder Werbenetzwerke (z.B. Meta Ads, TikTok Ads). Die in die Plattform integrierten SDKs sind:

- **Firebase Analytics:** Sammelt nur anonymisierte Nutzungsstatistiken. Erfasste Ereignisse beschränken sich auf App-Starts, Bildschirmansichtszeiten, Absturzberichte und Erfolgs-/Fehlerquoten im Kaufablauf.
- **Firebase App Check / Crashlytics:** Ihr Gerätemodell und Ihre Betriebssystemversion werden verwendet, um technische Fehler zu erkennen und unbefugten Zugriff zu verhindern.

5. Benachrichtigungs- und Ankündigungsinfrastruktur

- **Standardnutzer:** Unsere Anwendung verwendet die Push-Benachrichtigungsinfrastruktur, um Standardnutzern (Kunden) sofort neue Kampagnen, Squad-Einladungen und Freundschaftsanfragen zuzustellen. Zu diesem Zweck wird ein anonymes Benachrichtigungs-Token Ihres Geräts verarbeitet. Sie können diese Benachrichtigungen jederzeit in den Betriebssystemeinstellungen Ihres Geräts deaktivieren.
- **Geschäftskonten:** Allgemeine Informationen und Ankündigungen des Plattformmanagements an Geschäftskonten werden nicht über die Push-Benachrichtigungsinfrastruktur, sondern direkt über das Panel „In-App-Nachricht/Ankündigung“ im Store-Profil angezeigt. Diese In-App-Ankündigungen sind Teil des Plattformdienstes und funktionieren unabhängig von den allgemeinen Benachrichtigungsberechtigungen des Geräts.

6. Profilauffindbarkeit und soziale Interaktion

Beiträge und Ereignisse, die von Nutzern geteilt werden, sind standardmäßig mit hoher Privatsphäre geschützt und können nur von Personen auf der genehmigten Freundesliste eingesehen werden. Dritte, die nicht auf Ihrer Freundesliste stehen, können nicht direkt auf Ihre persönlichen Inhalte zugreifen.

- **Auffindbarkeit:** Aufgrund der sozialen Natur der Plattform sind Ihre Biografie und Ihre Freundesliste (mit wem Sie verbunden sind) auf der Plattform sichtbar, um das Schließen neuer Freundschaften zu erleichtern.
- **Gemeinsame Interaktionen:** Wenn Sie einen von einem Freund geteilten Beitrag kommentieren oder an dessen Veranstaltung teilnehmen, können diese Interaktionen von anderen gemeinsamen Kontakten (auch wenn Sie keine Freunde sind) gesehen werden, die berechtigt sind, diesen Inhalt zu sehen.

7. Nachrichten-Datenschutz und technische Sicherheit

Die Inhalte der Eins-zu-Eins-Nachrichten werden ausschließlich zum Zweck der Übermittlung zwischen den Parteien verarbeitet. Nachrichtenhinhalte können standardmäßig in keiner Weise vom Plattformpersonal oder -management gelesen oder eingesehen werden. Sicherheits-, Spam- und Missbrauchskontrollen werden vom System durch eine begrenzte und automatisierte Metadatenanalyse durchgeführt, nicht durch das Lesen von Nachrichteninhalten.

8. Algorithmus für die Inhaltsanzeige

Die Anzeige von Inhalten wird in zwei verschiedenen Bereichen algorithmisch gesteuert:

- **Feed (Sozial):** Nur die Inhalte von genehmigten Freunden werden in chronologischer Reihenfolge und nach Interaktion angezeigt.
- **Angebotsseite und Karte:** Bezahlte (Token-)Kampagnen von Unternehmen werden durch einen transparenten Algorithmus eingestuft, der auf dem Standort des Nutzers, dem Verfolgen des Geschäfts, der Priorität spezieller Kampagnenvorlagen wie Flash

Sale (20% Rabatt und mehr) und einer dynamischen Bewertungszahl basiert, die sich auf organische Interaktionsraten der Kampagne (Aufrufe, Klicks, Nutzung) stützt.

9. Inhaltsmoderation, Sanktionen und Einspruch

Um ein sicheres Community-Umfeld zu gewährleisten, durchlaufen geteilte Inhalte einen dynamischen Profanitätsfilter (Schimpfwörter/Beleidigungen) auf Serverseite. Bei Verstoß gegen die Regeln werden folgende Sanktionen angewendet:

- **Vorübergehende Sperrung:** Bei wiederholtem Verstoß wird das Konto für einen bestimmten Zeitraum eingeschränkt.
- **Dauerhafte Sperrung (Permanent Ban):** Bei Feststellung von Betrug, Belästigung, gefälschtem Standort (Mock GPS) oder richtlinienverletzendem Verhalten wird das Konto dauerhaft gelöscht.
- **Einspruch (Appeal):** Nutzer haben das Recht, innerhalb von 14 Tagen über jorbiapp@gmail.com eine menschliche Überprüfung (SLA: 48 Stunden) bezüglich Moderationsentscheidungen anzufordern.

10. Internationale Datenübermittlung

Die Jorbi-Infrastruktur läuft überwiegend bei globalen Dienstanbietern mit Sitz in den USA und der EU. In Übereinstimmung mit Artikel 9 KVKK und den DSGVO-Datenübermittlungsregeln werden unter Berücksichtigung des Prinzips der Datenminimierung nur die für den jeweiligen Dienst erforderlichen Mindestdaten an die folgenden Anbieter übermittelt:

Dienstanbieter (Land)	**Kategorie der übermittelten Daten und Nutzungszweck**
Google Firebase / GCP (USA / EU)	Authentifizierung (Auth), Nutzerprofile, Nachrichten und Beiträge (Firestore/Storage), analytische Statistiken und Absturzprotokolle.
Google Maps Platform (USA / EU)	Nur sofortige Standortkoordinaten (GPS) und regionale Kampagnen-Kartierungsdaten.
RevenueCat (USA)	Protokolle von In-App-Käufen (Ticket/Token) und Daten zur Bestätigung der digitalen Berechtigung (Kartendaten werden niemals übermittelt).
Apple App Store &	Protokolle zur Überprüfung der Gerätesicherheit (App Attest /

Dienstanbieter (Land)	Kategorie der übermittelten Daten und Nutzungszweck
Google Play (USA)	Play Integrity) und anonyme Rechnungsfreigaben.

Alle diese Übermittlungen erfolgen unter der Zusicherung von DSGVO-konformen Standardvertragsklauseln (SCC) und ISO 27001-Sicherheitszertifikaten.

11. Gesetzliche Anfragen und Strafverfolgungsbehörden

Jorbi räumt dem Schutz der Privatsphäre der Nutzer Priorität ein. Im Falle einer ordnungsgemäßen, verbindlichen und rechtmäßigen Anfrage von offiziellen Behörden (Gerichte, Staatsanwaltschaften, autorisierte Polizeieinheiten) können die angeforderten Mindestdaten jedoch an die zuständigen Behörden weitergegeben werden, um unseren rechtlichen Verpflichtungen gemäß den geltenden Gesetzen nachzukommen.

12. Datenaufbewahrungsfristen und inaktive Konten (TTL)

Gemäß der Datenminimierung gelten folgende Fristen für die automatische Löschung (TTL):

- **Eins-zu-Eins-Nachrichten:** Werden nach 90 Tagen dauerhaft gelöscht.
- **Benachrichtigungen:** Werden nach 30 Tagen automatisch gelöscht.
- **Kurzzeitaktivitäten:** Werden 2 Stunden nach dem Teilen aus dem System entfernt.
- **Ticket- und Sitzungsprotokolle:** Werden zur Transaktionssicherheit nach 48 Stunden gelöscht.
- **Kampagnendaten:** Abgelaufene oder vom Geschäft geschlossene Kampagnen werden nach 8 Tagen im Einklang mit dem Prinzip der Datenminimierung dauerhaft aus der Datenbank gelöscht.
- **Team-/Gruppendaten (Squad):** Erfolgreich abgeschlossene Gruppendaten werden nach 7 Tagen vollständig aus dem System gelöscht, unvollständige (abgebrochene) nach 3 Tagen.
- **Menschliche Interaktion und Markierung (Tag):** Wenn Nutzer in ihren Beiträgen Geschäfte markieren (@geschäft), kann dieser Inhalt in das Geschäftsprofil übertragen werden. Der Nutzer wird über diese Situation vor dem Teilen des Beitrags ausdrücklich durch eine In-App-Warnung informiert. Zum Schutz der Privatsphäre werden Nutzernamen maskiert (z.B. „jo...“). Diese Daten bleiben nicht dauerhaft im Geschäftsprofil und werden jeden Morgen um 08:00 Uhr automatisch gelöscht.
- **Inaktive Konten:** Standard-Nutzerkonten, in die 24 Monate lang ununterbrochen nicht eingeloggt wurde und die in einen inaktiven (passiven) Zustand übergegangen sind, werden dauerhaft und automatisch aus dem System gelöscht.

13. Kontolöschung, Recht auf Vergessenwerden und Datenübertragbarkeit

- **Kontolöschung:** Sie können Ihr Konto über das Menü Einstellungen > Mein Konto löschen in der Anwendung oder über die Adresse jorbi.app/delete-account löschen.

- **Standardnutzer:** Wenn der Löschvorgang eingeleitet wird, werden alle personenbezogenen Daten sofort und dauerhaft gelöscht.
- **Geschäftskonten (Store):** Um wiederholten Missbrauch von Willkommens-Token zu verhindern, werden E-Mail, Telefonnummer und Geräte-ID durch einseitiges Hashing mittels SHA-256 gespeichert. Sie werden 180 Tage lang in gesperrchten Sicherheitsprotokollen aufbewahrt. Nach Ablauf der 180 Tage werden sie vollständig vernichtet.
- **Lizenzdauer für nutzergenerierte Inhalte (UGC):** Für den Fall, dass der Nutzer sein Konto löscht oder die entsprechenden Inhalte entfernt, erlöschen die Lizenz und die Nutzungsrechte an diesen Inhalten erst am Ende eines angemessenen Zeitraums, der für technische Backup-Prozesse erforderlich ist.
- **Datenübertragbarkeit:** Sie können eine maschinenlesbare Kopie Ihrer Daten (im JSON- oder CSV-Format) über jorbiapp@gmail.com anfordern. Ihre Anfrage wird spätestens innerhalb von 30 Tagen bearbeitet.

14. Verfahren bei Datenschutzverletzungen (Data Breach)

Jorbi verwendet branchenübliche Verschlüsselung und Firewalls zum Schutz Ihrer Daten. Im Falle der Feststellung eines unbefugten Zugriffs, Cyberangriffs oder Datenlecks (Data Breach) werden die betroffenen Nutzer und die zuständigen Datenschutzbehörden (KVKK/DSGVO DPA) innerhalb von maximal 72 Stunden transparent per E-Mail informiert.

15. Kindersicherheit und Altersgrenze

Sie müssen mindestens 18 Jahre alt sein, um die Jorbi-Plattform nutzen zu können. In der Registrierungsphase wird diese Bedingung durch eine Altersverifikationserklärung eingeholt. Die Plattform sammelt nicht wissentlich Daten von Kindern unter 18 Jahren. Wird festgestellt oder gemeldet, dass ein Konto einer Person unter 18 Jahren gehört, werden das betreffende Konto und alle zugehörigen Daten umgehend gelöscht. Eltern können verdächtige Situationen über unseren Kommunikationskanal melden.

16. Richtlinienänderungen und Kontakt

Jorbi behält sich das Recht vor, diese Datenschutzrichtlinie zu aktualisieren. Wichtige Änderungen werden über In-App-Benachrichtigungen bekannt gegeben. Für alle Anfragen und Einwände bezüglich Ihrer Privatsphäre, Datenübertragbarkeit und KVKK/DSGVO-Rechte:

E-Mail: jorbiapp@gmail.com