Política de Privacidad y Texto Informativo de JORBI

Versión: 1.0 | **Última Actualización:** Mayo de 2026

Nombre de la Aplicación: Jorbi (la "Aplicación" o la "Plataforma")

Jorbi otorga la máxima importancia a la privacidad de sus usuarios y a la protección de sus datos personales. Al descargar o utilizar la Aplicación, se considera que usted ha aceptado esta Política de Privacidad. Esta política ha sido elaborada bajo el principio de "Privacy by Design" (Privacidad desde el Diseño), teniendo en cuenta la KVKK (Turquía), el RGPD (UE) y las normativas internacionales de protección de datos aplicables.

1. Responsable del Tratamiento y Datos de Contacto

- **Responsable del Tratamiento (Nombre / Razón Social):** Çiğdem Ertek Mutlu
- **Número de Identificación Fiscal:** 33154498546
- **Dirección de Notificación Legal:** Akarbaşı Mah. Ada Sk. Prestij Konutları C D Blok C Blok No: 33 İç Kapı No: 6 Odunpazarı / Eskişehir, Turquía
- **Contacto de Privacidad y KVKK (Privacy Contact):** jorbiapp@gmail.com

2. Declaración de Datos Sensibles (Datos no tratados)

Jorbi no tiene como finalidad recopilar, ni solicita que se proporcionen, Datos Personales de Categoría Especial (Sensibles) tales como raza, origen étnico, opiniones políticas, creencias religiosas, vestimenta, afiliación a asociaciones/fundaciones, salud, vida sexual o datos biométricos/genéticos.

3. Datos Recopilados, Fines del Tratamiento y Base Legal (Matriz)

Los datos mínimos recopilados requeridos para el funcionamiento de la Aplicación, sus propósitos y sus bases legales se enumeran de forma transparente a continuación:

Categoría de Datos	**Finalidad del Tratamiento**	**Base Legal (KVKK / GDPR)**
Identidad (Nombre, Apellido, Nombre de usuario)	Creación de cuenta, interacción social dentro de la plataforma.	Establecimiento y Ejecución del Contrato
Contacto (Correo electrónico)	Seguridad de la cuenta, restablecimiento de contraseña, notificaciones legales obligatorias.	Ejecución del Contrato / Interés Legítimo

Categoría de Datos	Finalidad del Tratamiento	Base Legal (KVKK / GDPR)
Número de Teléfono (Solo Tiendas)	Verificación de cuenta comercial (Tienda) y seguridad OTP.	Ejecución del Contrato / Interés Legítimo
Medios (Cámara y galería)	Carga de foto de perfil y uso compartido de imágenes de publicaciones/eventos.	Consentimiento Expreso (Permiso del dispositivo)
Contenido del Usuario (Publicaciones, Comentarios)	Proporcionar infraestructura de socialización e interacción mutua dentro de la plataforma.	Ejecución del Contrato
Datos de Mensajería	Garantizar una comunicación segura uno a uno entre usuarios.	Ejecución del Contrato
Ubicación (GPS en primer plano)	Visualización de ofertas regionales y validación de boletos de distancia de la tienda (150 m).	Consentimiento Expreso
ID del Dispositivo (Con hash)	Prevención del abuso de promociones duplicadas (Solo Tiendas).	Interés Legítimo del Responsable del Tratamiento
Datos de Red y Conexión (Dirección IP)	Ciberseguridad, obligaciones de registro, prevención de registros comerciales falsos y abusos.	Interés Legítimo
Financiero (Registros de Compras)	Asignación de derechos de token/moneda (entitlement) a la cuenta.	Ejecución del Contrato / Obligación Legal

Categoría de Datos	Finalidad del Tratamiento	Base Legal (KVKK / GDPR)
Análisis y Registros de Fallas	Medición de la estabilidad de la aplicación, resolución de errores de falla.	Interés Legítimo

- **Datos de Enriquecimiento de Perfil:** La ciudad de residencia, los intereses y la información de la biografía, proporcionados de forma totalmente voluntaria (opcional) por el usuario, se procesan bajo el alcance del Consentimiento Expreso para enriquecer la estructura social.

Explicaciones Detalladas sobre los Fines del Tratamiento de Datos:

- **Ejecución del Contrato:** Para que los usuarios estándar (clientes) se beneficien de las campañas y ofertas de la plataforma sin problemas; y para que las cuentas comerciales (tiendas) puedan comprar tokens, crear, planificar y publicar campañas, cumpliendo con las obligaciones contractuales entre las partes.
- **Verificación Basada en la Ubicación:** Confirmar la distancia física entre el usuario y la tienda para evitar el abuso de las ofertas.
- **Seguridad y Prevención de Abusos:** Prevención de aplicaciones de ubicaciones falsas (Mock GPS) y protección de la integridad comercial de la plataforma. En este contexto, se operan algoritmos de geovallas (*Geofencing*) y radares automáticos de cuarentena para evitar que cuentas previamente restringidas por violaciones de políticas vuelvan a infiltrarse en la plataforma con diferentes cuentas utilizando sus números de teléfono o identificaciones de dispositivo (Device ID).

4. SDK de Terceros, Análisis y Cookies

Jorbi no realiza ningún perfilado publicitario (Ad Tracking) dirigido a los usuarios y no vende sus datos a corredores de datos (Data Brokers) ni a redes publicitarias (Ej: Meta Ads, TikTok Ads). Las integraciones de SDK aplicadas en la plataforma son las siguientes:

- **Firebase Analytics:** Solo recopila estadísticas de uso anonimizadas. Los eventos recopilados se limitan a la apertura de la aplicación, los tiempos de visualización de la pantalla, los informes de fallos (crash) y las tasas de éxito/error del flujo de compra.
- **Firebase App Check / Crashlytics:** El modelo de su dispositivo y la versión del sistema operativo se utilizan para la detección de errores técnicos y la prevención de accesos no autorizados.

5. Infraestructura de Notificaciones y Anuncios

- **Usuarios Estándar:** Nuestra aplicación utiliza la infraestructura de notificaciones emergentes (Push Notifications) para transmitir instantáneamente nuevas campañas, invitaciones de equipo (squad) y solicitudes de amistad a los usuarios estándar (clientes), y para este propósito se procesa un token de notificación anónimo perteneciente a su dispositivo. Puede desactivar estas notificaciones en cualquier momento desde la configuración del sistema operativo de su dispositivo.
- **Cuentas de Tienda (Store):** Las informaciones generales y los anuncios realizados por la administración de la plataforma a las cuentas comerciales no se envían a través de la infraestructura de notificaciones emergentes, sino que se muestran directamente dentro del perfil de la tienda a través del panel de 'mensajes/anuncios en la aplicación'. Estos anuncios dentro de la aplicación son parte del servicio de la plataforma y funcionan independientemente de los permisos de notificación generales del dispositivo.

6. Descubrimiento de Perfiles e Interacción Social

Las publicaciones y los eventos compartidos por los usuarios están protegidos con un alto nivel de privacidad por defecto y solo pueden ser vistos por las personas en la lista de amigos aprobada. Terceros que no estén en su lista de amigos no pueden acceder directamente a su contenido personal.

- **Descubrimiento:** Debido a la naturaleza social de la plataforma; su biografía y su lista de amigos (con quién está conectado) son visibles en la plataforma para facilitar el establecimiento de nuevas amistades.
- **Interacciones Mutuas:** Cuando usted comenta una publicación compartida por un amigo o asiste a su evento, estas interacciones pueden ser vistas por otras conexiones mutuas que estén autorizadas a ver dicho contenido (incluso si no son amigos suyos).

7. Privacidad de Mensajería y Seguridad Técnica

Los contenidos de la mensajería individual se procesan únicamente con el fin de transmisión entre las partes. Por defecto, los contenidos de los mensajes son estrictamente ilegibles y no pueden ser vistos por el personal o la administración de la plataforma. Los controles de seguridad, spam y abuso no se llevan a cabo mediante la lectura del contenido de los mensajes, sino a través de un análisis de metadatos (rastros de datos) automático y limitado gestionado por el sistema.

8. Algoritmo de Visualización de Contenido

La visualización de contenidos se gestiona algorítmicamente en dos áreas diferentes:

- **Feed (Social):** Solo se muestran los contenidos de los amigos aprobados según el tiempo y el orden de interacción.
- **Página de Ofertas y Mapa:** Las campañas pagadas (con tokens) de las empresas; se ordenan mediante un algoritmo transparente basado en la ubicación del usuario, si sigue o no a la tienda, la prioridad de plantillas de campañas especiales como las Ofertas Flash (20% de descuento o más), y una puntuación de evaluación dinámica

basada en las tasas de interacción orgánica (visualizaciones, clics, usos) de la campaña.

9. Moderación de Contenido, Sanciones y Apelación

Para garantizar un entorno comunitario seguro, los contenidos compartidos pasan a través de un filtro dinámico de obscenidad (insultos/ofensas) del lado del servidor. En caso de violación de las reglas, se aplican las siguientes sanciones:

- **Suspensión Temporal (Temporary Suspension):** En caso de reincidencia, la cuenta queda restringida por un período de tiempo determinado.
- **Cierre Permanente (Permanent Ban):** En caso de fraude, acoso, ubicación falsa (Mock GPS) o detección por el radar de cuarentena, la cuenta se elimina permanentemente.
- **Apelación (Appeal):** Los usuarios tienen derecho a solicitar una revisión humana (SLA: 48 horas) contra las decisiones de moderación dentro de los 14 días enviando un correo a jorbiapp@gmail.com.

10. Transferencia Internacional de Datos

La infraestructura de Jorbi funciona principalmente en proveedores de servicios globales con sede en los EE. UU. y la UE. De acuerdo con el Artículo 9 de la KVKK y las normas de transferencia de datos del RGPD, considerando el principio de minimización de datos, solo se transfieren a los siguientes proveedores los datos mínimos requeridos por el servicio correspondiente:

Proveedor de Servicios (País)	**Categoría de Datos Transferidos y Finalidad de Uso**
Google Firebase / GCP (EE. UU. / UE)	Autenticación (Auth), perfiles de usuario, mensajes y publicaciones (Firestore/Storage), estadísticas analíticas y registros de fallos.
Google Maps Platform (EE. UU. / UE)	Únicamente coordenadas de ubicación instantánea (GPS) y datos de mapeo de campañas regionales.
RevenueCat (EE. UU.)	Registros de compras dentro de la aplicación (entradas/tokens) y datos de validación de derechos digitales (*entitlement*) (La información de las tarjetas nunca se transfiere).

Proveedor de Servicios (País)	Categoría de Datos Transferidos y Finalidad de Uso
Apple App Store & Google Play (EE. UU.)	Registros de validación de seguridad del dispositivo (App Attest / Play Integrity) y confirmaciones de facturación anónimas.

Todas estas transferencias se realizan bajo la garantía de las Cláusulas Contractuales Tipo (SCC) compatibles con el RGPD y los certificados de seguridad ISO 27001.

11. Solicitudes Legales y Fuerzas del Orden

Jorbi basa sus principios en la privacidad del usuario. Sin embargo, en el caso de una solicitud legal, vinculante y debidamente formalizada por parte de las autoridades oficiales (Tribunales, Fiscalías, unidades policiales autorizadas), los datos mínimos solicitados podrán ser compartidos con las autoridades competentes con el fin de cumplir con nuestras obligaciones legales bajo las leyes vigentes.

12. Períodos de Retención de Datos y Cuentas Pasivas (TTL)

De acuerdo con la minimización de datos, los períodos de eliminación automática (TTL) son los siguientes:

- **Mensajes Individuales:** Se eliminan permanentemente después de 90 días.
- **Notificaciones:** Se limpian automáticamente después de 30 días.
- **Actividades a Corto Plazo:** Se eliminan del sistema 2 horas después de compartirlas.
- **Registros de Sesiones y Entradas:** Se eliminan después de 48 horas por motivos de seguridad en las transacciones.
- **Datos de Campaña:** Las campañas expiradas o cerradas por la tienda se eliminan permanentemente de la base de datos después de 8 días de acuerdo con el principio de minimización de datos de la plataforma.
- **Datos de Equipo / Grupo (Squad):** Los datos de los grupos completados con éxito se eliminan por completo del sistema después de 7 días, y los datos de los grupos no completados (cancelados) después de 3 días.
- **Interacción Humana y Etiquetado (Tag):** Cuando los usuarios etiquetan tiendas en sus publicaciones (@tienda), este contenido puede transferirse al perfil de la tienda. El usuario es informado explícitamente mediante una advertencia en la aplicación antes de compartir la publicación. Para proteger la privacidad, los nombres de usuario se muestran enmascarados (por ejemplo, "jo..."). Estos datos no son permanentes en el perfil de la tienda y se limpian automáticamente todas las mañanas a las 08:00.
- **Cuentas Pasivas:** Las cuentas de usuarios estándar que no han iniciado sesión de forma continua durante 24 meses y caen en un estado inactivo (pasivo) se eliminan de forma permanente y automática del sistema.

13. Eliminación de Cuenta, Derecho al Olvido y Portabilidad de Datos

- **Eliminación de Cuenta:** Puede eliminar su cuenta desde el menú Configuración > Eliminar mi cuenta dentro de la aplicación o a través de la dirección jorbi.app/delete-account.
- **Usuarios Estándar:** Cuando se inicia el proceso de eliminación, todos los datos personales se eliminan de forma instantánea y permanente.
- **Cuentas de Tienda (Store):** Para evitar el abuso duplicado de los tokens de bienvenida, el correo electrónico, el teléfono y la identificación del dispositivo se almacenan aplicando un hash unidireccional utilizando SHA-256. Estos se mantienen en registros de seguridad bloqueados durante 180 días. Al final de los 180 días, se destruyen por completo.
- **Portabilidad de Datos:** Puede solicitar una copia legible por máquina de sus datos (en formato JSON o CSV) a través de jorbiapp@gmail.com. Su solicitud será entregada en un plazo máximo de 30 días.

14. Procedimiento de Violación de Datos (Data Breach)

Jorbi utiliza cifrado estándar de la industria y cortafuegos para proteger sus datos. En caso de detectar cualquier acceso no autorizado, ataque cibernético o fuga de datos (Data Breach); los usuarios afectados y las autoridades de protección de datos competentes (KVKK/GDPR DPA) serán informados por correo electrónico y de forma transparente dentro de un plazo máximo de 72 horas.

15. Seguridad Infantil y Límite de Edad

Para utilizar la plataforma Jorbi es obligatorio tener al menos 18 años. Este requisito se obtiene con una declaración de verificación de edad durante el proceso de registro. La plataforma no recopila a sabiendas datos de menores de 18 años. Si se descubre o se denuncia que una cuenta pertenece a un menor de 18 años, la cuenta respectiva y todos sus datos se eliminarán inmediatamente. Los padres pueden informar situaciones sospechosas a través de nuestro canal de comunicación.

16. Cambios en la Política y Contacto

Jorbi se reserva el derecho de actualizar esta Política de Privacidad. Los cambios importantes se anunciarán a través de notificaciones dentro de la aplicación.

Para todas sus solicitudes y objeciones relacionadas con la privacidad, la portabilidad de datos y sus derechos bajo KVKK/RGPD: **Correo electrónico:** jorbiapp@gmail.com