Politique de Confidentialité et Texte d'Information de JORBI

Version : 1.0 | Dernière mise à jour : Juin 2026

Nom de l'application : Jorbi ("Application" ou "Plateforme")

Jorbi attache la plus haute importance à la confidentialité de ses utilisateurs et à la protection de leurs données personnelles. En téléchargeant ou en utilisant l'Application, vous êtes réputé avoir accepté cette Politique de Confidentialité. Cette politique a été préparée selon le principe du "Privacy by Design" (Confidentialité dès la conception), en tenant compte de la KVKK (Turquie), du RGPD (UE) et des réglementations internationales applicables en matière de protection des données.

1. Responsable du traitement des données et Coordonnées

- **Responsable du traitement (Nom / Titre) :** Çiğdem Ertek Mutlu
- **N° d'identification fiscale :** 33154498546
- **Adresse de notification légale :** Akarbaşı Mah. Ada Sk. Prestij Konutları C D Blok C Blok No: 33 İç Kapı No: 6 Odunpazarı / Eskişehir, Turquie
- **Contact Confidentialité et KVKK :** jorbiapp@gmail.com

2. Déclaration sur les données sensibles (Données non traitées)

Jorbi ne vise pas à traiter et ne demande pas la fourniture de Catégories Particulières de Données à Caractère Personnel (Données Sensibles) telles que la race, l'origine ethnique, les opinions politiques, les convictions religieuses, l'habillement, l'appartenance syndicale/associative, la santé, la vie sexuelle ou les données biométriques/génétiques.

3. Données collectées, Finalités du traitement et Base juridique (Matrice)

Les données minimales collectées en raison du fonctionnement de l'application, leurs finalités et les bases juridiques sont listées de manière transparente ci-dessous :

Catégorie de données	**Finalité du traitement**	**Base juridique (KVKK / RGPD)**
Identité (Nom, Prénom, Nom d'utilisateur)	Création de compte, interaction sociale au sein de la plateforme.	Exécution d'un contrat
Contact (E-mail)	Sécurité du compte, réinitialisation du mot de passe, notifications légales obligatoires.	Exécution d'un contrat / Intérêt légitime

Catégorie de données	**Finalité du traitement**	**Base juridique (KVKK / RGPD)**
Numéro de téléphone (Commerces uniquement)	Vérification du compte commercial (Boutique) et sécurité OTP.	Exécution d'un contrat / Intérêt légitime
Médias (Appareil photo et galerie)	Téléchargement de la photo de profil et partage de visuels de publications/événements.	Consentement explicite (Autorisation de l'appareil)
Contenu Utilisateur (Publications, Commentaires)	Fourniture de la socialisation sur la plateforme et infrastructure d'interaction mutuelle.	Exécution d'un contrat
Données de messagerie	Garantir une communication sécurisée de personne à personne entre les utilisateurs.	Exécution d'un contrat
Localisation (GPS au premier plan)	Affichage des opportunités régionales et approbation des tickets par distance du commerce (150m).	Consentement explicite
Identifiant de l'appareil (Haché)	Prévention de l'abus de promotions en double (Commerces uniquement).	Intérêt légitime du Responsable du traitement
Données de réseau et de connexion (Adresse IP)	Cybersécurité, obligations de journalisation, prévention des fausses inscriptions d'entreprises et des abus.	Intérêt légitime

Catégorie de données	Finalité du traitement	Base juridique (KVKK / RGPD)
Financier (Journaux d'achat)	Définition du droit de jeton/token (entitlement) sur le compte.	Exécution d'un contrat / Obligation légale
Analytique et Journaux de plantage	Mesure de la stabilité de l'application, correction des erreurs de plantage (crash).	Intérêt légitime

Données d'enrichissement du profil : Les informations telles que la ville de résidence, les intérêts et la biographie, fournies entièrement à la propre demande de l'utilisateur (facultatif), sont traitées sous le Consentement Explicite afin d'enrichir la structure sociale.

Explications détaillées sur les finalités du traitement des données :

- **Exécution du Contrat :** Remplir les obligations contractuelles entre les parties afin que les utilisateurs standards (clients) puissent bénéficier sans problème des campagnes et des opportunités sur la plateforme ; et que les comptes commerciaux (boutiques) puissent acheter des jetons, créer, planifier et publier des campagnes.
- **Vérification basée sur la localisation :** Confirmer la distance physique entre l'utilisateur et le commerce pour éviter l'abus des opportunités.
- **Sécurité et prévention des abus :** Prévenir les applications de fausse localisation (Mock GPS) et protéger l'intégrité commerciale de la plateforme. Dans ce contexte, afin d'empêcher les comptes précédemment restreints pour violation des politiques de s'infiltrer à nouveau sur la plateforme avec des comptes différents utilisant les mêmes numéros de téléphone ou identifiants d'appareils, des algorithmes de sécurité détectant les comptes violant les règles (policy-violating) et le gardiennage virtuel (Geofencing) sont mis en œuvre.

4. SDK tiers, Analytique et Cookies

Jorbi ne procède à aucun profilage publicitaire (Ad Tracking) dirigé vers les utilisateurs et ne vend pas vos données à des courtiers en données ou à des réseaux publicitaires (ex. Meta Ads, TikTok Ads). Les intégrations SDK appliquées sur la plateforme sont :

- **Firebase Analytics :** Collecte uniquement des statistiques d'utilisation anonymisées. Les événements collectés se limitent à l'ouverture de l'application, aux temps d'affichage à l'écran, aux rapports de plantage (crash) et aux taux de réussite/d'erreur dans le flux d'achat.

- **Firebase App Check / Crashlytics :** Le modèle de votre appareil et la version de votre système d'exploitation sont utilisés pour détecter les erreurs techniques et empêcher les accès non autorisés.

5. Infrastructure de notifications et d'annonces

- **Utilisateurs Standards :** Notre application utilise l'infrastructure de notifications Push pour transmettre instantanément de nouvelles campagnes, des invitations d'équipe (squad) et des demandes d'amis aux utilisateurs standards (clients), et un jeton de notification anonyme appartenant à votre appareil est traité à cette fin. Vous pouvez désactiver ces notifications à tout moment depuis les paramètres du système d'exploitation de votre appareil.
- **Comptes commerciaux :** Les informations générales et les annonces faites par la direction de la plateforme aux comptes commerciaux ne sont pas affichées via l'infrastructure de notifications push, mais directement via le panneau "message/annonce intégrée à l'application" au sein du profil du commerce. Ces annonces intégrées à l'application font partie du service de la plateforme et fonctionnent indépendamment des autorisations de notification générales de l'appareil.

6. Découvrabilité du profil et interaction sociale

Les publications et les événements partagés par les utilisateurs sont protégés par défaut par un niveau élevé de confidentialité et ne peuvent être vus que par les personnes figurant sur la liste d'amis approuvée. Les tiers qui ne figurent pas sur votre liste d'amis ne peuvent pas accéder directement à votre contenu personnel.

- **Découvrabilité :** En raison de la nature sociale de la plateforme, votre biographie et votre liste d'amis (avec qui vous êtes connecté) sont visibles sur la plateforme afin de faciliter la création de nouvelles amitiés.
- **Interactions mutuelles :** Lorsque vous commentez une publication partagée par un ami ou participez à son événement, ces interactions peuvent être vues par d'autres connexions communes (même si vous n'êtes pas amis) qui sont autorisées à voir ce contenu.

7. Confidentialité de la messagerie et sécurité technique

Le contenu de la messagerie de personne à personne est traité uniquement à des fins de transmission entre les parties. Par défaut, le contenu des messages ne peut absolument pas être lu ou consulté par le personnel ou la direction de la plateforme. Les contrôles de sécurité, de spam et d'abus sont effectués par le système via une analyse de métadonnées limitée et automatisée, et non par la lecture du contenu des messages.

8. Algorithme d'affichage du contenu

L'affichage du contenu est géré algorithmiquement dans deux domaines différents :

- **Flux (Social) :** Seuls les contenus des amis approuvés sont affichés par ordre chronologique et d'interaction.
- **Page des Opportunités et Carte :** Les campagnes payantes (avec jetons) des entreprises sont classées par un algorithme transparent basé sur l'emplacement de

l'utilisateur, le fait qu'il suive ou non le commerce, la priorité des modèles de campagne spéciaux tels que la Vente Flash (20% de réduction ou plus), et un score d'évaluation dynamique basé sur les taux d'interaction organique de la campagne (vues, clics, utilisation).

9. Modération du contenu, Sanctions et Appel

Pour garantir un environnement communautaire sûr, les contenus partagés passent par un filtre dynamique de blasphème (insultes/gros mots) côté serveur. En cas de violation des règles, les sanctions suivantes sont appliquées :

- **Suspension temporaire :** En cas de récidive, le compte est restreint pour une certaine période.
- **Bannissement permanent (Permanent Ban) :** En cas de détection de fraude, de harcèlement, de fausse localisation (Mock GPS) ou de violation des règles, le compte est définitivement supprimé.
- **Appel (Appeal) :** Les utilisateurs ont le droit de demander un examen humain (SLA : 48 heures) concernant les décisions de modération dans un délai de 14 jours à l'adresse jorbiapp@gmail.com.

10. Transfert international de données

L'infrastructure de Jorbi fonctionne principalement sur des fournisseurs de services mondiaux basés aux États-Unis et dans l'UE. Conformément à l'Article 9 de la KVKK et aux règles de transfert de données du RGPD, en tenant compte du principe de minimisation des données, seules les données minimales requises par le service concerné sont transférées aux fournisseurs suivants :

Fournisseur de services (Pays)	**Catégorie de données transférées et finalité de l'utilisation**
Google Firebase / GCP (États-Unis / UE)	Authentification (Auth), profils d'utilisateurs, messages et publications (Firestore/Storage), statistiques analytiques et journaux de plantage.
Google Maps Platform (États-Unis / UE)	Uniquement les coordonnées de localisation instantanée (GPS) et les données de cartographie des campagnes régionales.
RevenueCat (États-Unis)	Journaux des achats intégrés (billet/jeton) et données de vérification des droits numériques (Les données de la carte ne sont jamais transférées).

Fournisseur de services (Pays)	Catégorie de données transférées et finalité de l'utilisation
Apple App Store & Google Play (États-Unis)	Journaux de vérification de la sécurité de l'appareil (App Attest / Play Integrity) et approbations de facturation anonymes.

Toutes ces transmissions sont effectuées sous la garantie de Clauses Contractuelles Types (CCT/SCC) conformes au RGPD et de certificats de sécurité ISO 27001.

11. Demandes légales et forces de l'ordre

Jorbi accorde la priorité à la confidentialité des utilisateurs. Toutefois, en cas de demande régulière, contraignante et légale émanant des autorités officielles (Tribunaux, Parquets, unités de police autorisées), les données minimales demandées peuvent être partagées avec les autorités compétentes afin de remplir nos obligations légales en vertu des lois en vigueur.

12. Périodes de conservation des données et Comptes inactifs (TTL)

Conformément à la minimisation des données, les périodes de suppression automatique (TTL) sont les suivantes :

- **Messages de personne à personne :** Définitivement supprimés après 90 jours.
- **Notifications :** Automatiquement effacées après 30 jours.
- **Activités à court terme :** Retirées du système 2 heures après avoir été partagées.
- **Journaux de tickets et de sessions :** Supprimés après 48 heures pour la sécurité des transactions.
- **Données de campagne :** Les campagnes ayant expiré ou ayant été fermées par le commerce sont définitivement supprimées de la base de données après 8 jours, conformément au principe de minimisation des données.
- **Données d'équipe / Groupe (Squad) :** Les données des groupes terminés avec succès sont complètement effacées du système après 7 jours, et les données incomplètes (annulées) après 3 jours.
- **Interaction humaine et Identification (Tag) :** Lorsque les utilisateurs identifient des commerces (@commerce) dans leurs publications, ce contenu peut être transféré vers le profil du commerce. L'utilisateur est explicitement informé de cette situation par un avertissement dans l'application avant de partager la publication. Pour protéger la confidentialité, les noms d'utilisateurs sont masqués (ex. "jo..."). Ces données ne sont pas permanentes sur le profil du commerce et sont automatiquement effacées tous les matins à 08h00.
- **Comptes inactifs :** Les comptes d'utilisateurs standards qui n'ont pas été connectés de manière ininterrompue pendant 24 mois et qui sont tombés dans un état inactif (passif) sont supprimés de manière permanente et automatique du système.

13. Suppression de compte, Droit à l'oubli et Portabilité des données

- **Suppression de compte :** Vous pouvez supprimer votre compte à partir du menu Paramètres > Supprimer mon compte dans l'application ou via l'adresse jorbi.app/delete-account.
- **Utilisateurs standards :** Lorsque le processus de suppression est lancé, toutes les données personnelles sont supprimées instantanément et définitivement.
- **Comptes commerciaux (Store) :** Pour éviter les abus répétés de jetons de bienvenue, l'e-mail, le numéro de téléphone et l'identifiant de l'appareil sont stockés en utilisant un hachage unidirectionnel (SHA-256). Ils sont conservés dans des journaux de sécurité verrouillés pendant 180 jours. Ils sont complètement détruits à l'issue de ces 180 jours.
- **Durée de licence du contenu généré par l'utilisateur (UGC) :** Dans le cas où l'utilisateur supprime son compte ou retire le contenu concerné, la licence et les droits d'utilisation de ces contenus n'expireront qu'à la fin d'une période raisonnable requise par les processus de sauvegarde technique.
- **Portabilité des données :** Vous pouvez demander une copie lisible par machine de vos données (au format JSON ou CSV) via jorbiapp@gmail.com. Votre demande sera traitée dans un délai maximum de 30 jours.

14. Procédure en cas de violation de données (Data Breach)

Jorbi utilise un cryptage et des pare-feu conformes aux normes de l'industrie pour protéger vos données. En cas de détection d'un accès non autorisé, d'une cyberattaque ou d'une fuite de données (Data Breach), les utilisateurs concernés et les autorités de protection des données compétentes (KVKK/RGPD DPA) seront informés de manière transparente par e-mail dans un délai maximum de 72 heures.

15. Sécurité des enfants et limite d'âge

Vous devez avoir au moins 18 ans pour utiliser la plateforme Jorbi. Lors de la phase d'inscription, cette condition est obtenue par une déclaration de vérification de l'âge. La plateforme ne collecte pas sciemment de données auprès d'enfants de moins de 18 ans. S'il est détecté ou signalé qu'un compte appartient à une personne de moins de 18 ans, le compte concerné et toutes ses données seront immédiatement supprimés. Les parents peuvent signaler des situations suspectes via notre canal de communication.

16. Modifications de la politique et Contact

Jorbi se réserve le droit de mettre à jour cette Politique de Confidentialité. Les modifications importantes seront annoncées via des notifications intégrées à l'application. Pour toute demande ou objection concernant votre confidentialité, la portabilité de vos données et vos droits KVKK/RGPD :

E-mail : jorbiapp@gmail.com