

Comment Orbikal protège les données de votre entreprise

Document technique à destination des équipes IT, juridiques ou RGPD de nos clients et prospects.

Version du 27 juillet 2026

Ce document complète nos [Mentions légales & Politique de confidentialité](#) avec un niveau de détail technique, à l'usage des équipes qui évaluent Orbikal avant un déploiement en entreprise. Il décrit l'architecture de sécurité, l'accès aux données par notre équipe, nos sous-traitants et vos droits. En cas de différence entre ce document et nos Mentions légales, ces dernières font foi.

EN BREF

- ✓ **Chiffrement** au repos (AES-256-GCM) et en transit (TLS) sur toutes les données sensibles
- ✓ **Isolation stricte par organisation** au niveau de la base de données (Row Level Security), pas seulement au niveau applicatif
- ✓ **Accès en lecture seule** sur tous les comptes tiers que vous connectez : Orbikal ne peut rien publier ni modifier à votre place
- ✓ **Aucun accès humain de routine** à vos données : l'accès applicatif est entièrement automatisé

A RÔLES AU SENS DU RGPD

- Orbikal agit comme **sous-traitant** (article 28 du RGPD) pour les données issues de vos connecteurs marketing (Google, Meta, réseaux sociaux, emailing, avis clients, e-commerce, Stripe...) : ces données sont traitées selon vos instructions, dans le seul but de les afficher dans votre tableau de bord.
- Orbikal agit comme **responsable de traitement** pour les données de gestion de votre propre compte Orbikal (identifiants de connexion, facturation de votre abonnement).
- Une clause de sous-traitance dédiée figure à l'article 12 de nos CGV. Si votre entreprise a besoin d'un accord de sous-traitance (DPA) formel distinct, contactez-nous.

B ISOLATION MULTI-TENANT DES DONNÉES

- Base de données PostgreSQL (Supabase), avec **Row Level Security (RLS)** activé sur l'ensemble des tables contenant des données client.
- Chaque requête est scopée à l'organisation de l'utilisateur authentifié **au niveau de la base de données elle-même**, pas seulement au niveau de l'application : une erreur de code applicatif ne suffirait pas, à elle seule, à exposer les données d'une autre organisation.
- Au sein d'une même organisation, le contrôle des rôles (propriétaire / administrateur / membre en lecture seule) est appliqué côté serveur sur l'ensemble des routes d'API, pas uniquement dans l'interface.

C CHIFFREMENT

- Les jetons d'authentification (OAuth) et clés API des connecteurs tiers sont **chiffrés au repos avec l'algorithme AES-256-GCM** avant tout stockage en base.
- Ces secrets ne sont **jamais exposés côté navigateur** : aucun accès direct depuis le poste client, uniquement via nos serveurs applicatifs.
- Toutes les communications (entre votre navigateur et Orbikal, entre Orbikal et les API tierces) sont **chiffrées en transit (HTTPS/TLS)**.
- Aucune donnée de moyen de paiement (numéro de carte bancaire, etc.) ne transite ni n'est stockée par nos serveurs : la facturation de votre abonnement est intégralement déléguée à **Stripe**, certifié PCI-DSS niveau 1.

D ACCÈS EN LECTURE SEULE AUX PLATEFORMES QUE VOUS CONNECTEZ

- Chaque connecteur utilise des scopes OAuth **strictement en lecture** (par ex. `analytics.readonly` , `ads_read` , `user.info.stats` ...), jamais de droit d'écriture sur vos comptes tiers.
- Concrètement : Orbikal ne peut **ni publier de contenu, ni modifier une campagne, ni supprimer quoi que ce soit** sur les comptes Google, Meta, réseaux sociaux, emailing ou e-commerce que vous connectez.

- Le détail des scopes utilisés par chaque connecteur est documenté dans nos Mentions légales, section 4.

E ACCÈS DE L'ÉQUIPE ORBIKAL À VOS DONNÉES

- En fonctionnement normal, l'accès applicatif à vos données est **exclusivement automatisé**, au seul service de leur affichage dans votre compte.
- L'équipe Orbikal peut toutefois consulter individuellement vos données, en **lecture seule**, via un outil interne dédié, uniquement dans les cas suivants : une **demande de support explicite de votre part** (ticket d'assistance que vous avez vous-même ouvert), une obligation légale, ou un incident de sécurité.
- Cet outil interne applique des garde-fous techniques : **aucune modification, connexion ou déconnexion de connecteur n'est possible** pendant son utilisation (blocage d'écriture au niveau serveur), chaque accès est **limité à 45 minutes** et **journalisé** (organisation consultée, date).
- Comme pour tout service hébergé, l'infrastructure technique sous-jacente (base de données) reste par ailleurs, par nature, techniquement administrable par l'opérateur du service dans le cadre de la maintenance de la plateforme.

F SOUS-TRAITANTS TECHNIQUES ET LOCALISATION DES DONNÉES

Sous-traitant	Rôle	Localisation
Supabase	Base de données et authentification	Royaume-Uni (région AWS eu-west-2, Londres). Le Royaume-Uni bénéficie d'une décision d'adéquation de la Commission européenne, qui permet les transferts de données depuis l'UE sans garantie contractuelle supplémentaire.
Vercel	Hébergement applicatif	États-Unis
Groq	Moteur d'IA de l'assistant Mika : reçoit votre prénom, le nom et la description de votre entreprise, votre secteur, vos objectifs, ainsi que des statistiques marketing agrégées — jamais les données individuelles de vos propres clients	États-Unis
Brevo	Emails transactionnels et rapports PDF programmés	France
Stripe	Facturation et gestion de votre abonnement	États-Unis (certifié PCI-DSS niveau 1)

Aucune donnée n'est vendue, louée ou partagée à des fins commerciales ou publicitaires, ni utilisée pour entraîner des modèles d'intelligence artificielle.

6 CONSERVATION ET SUPPRESSION DES DONNÉES

- Les données issues de vos connecteurs sont conservées tant que le connecteur reste actif, pour permettre l'affichage continu du tableau de bord.
- À la déconnexion d'un connecteur, les identifiants d'accès (jetons OAuth, clés API) sont **supprimés immédiatement**.
- Vous pouvez supprimer votre compte Orbikal à tout moment (depuis les paramètres de votre compte, ou par email) : la suppression entraîne la suppression de l'ensemble des données associées (connecteurs, statistiques mises en cache, abonnement Stripe résilié).
- Pour les connecteurs Google, Meta, LinkedIn et TikTok, vous pouvez également révoquer l'accès directement depuis les paramètres de votre compte sur la plateforme concernée, ce qui invalide immédiatement les jetons côté fournisseur.

H VOS DROITS ET CONTACT

Conformément au RGPD, vous disposez des droits d'accès, de rectification, d'effacement, d'opposition et de portabilité (articles 15 à 20).

Pour exercer ces droits, ou pour toute question technique sur ce document, contactez **contact@orbikal.com** — réponse sous 30 jours maximum. Vous pouvez également introduire une réclamation auprès de la [CNIL](#).

Ce document a vocation informative et complète nos Mentions légales & Politique de confidentialité, qui font foi en cas de différence. Il sera mis à jour à mesure de l'évolution de nos connecteurs et sous-traitants.