

BULLS CRM **Dossier sécurité et RGPD**

Version du 22 octobre 2026 · bullaria.com/securite

En bref

BULLS CRM est le logiciel de prospection et de gestion commerciale de Bullaria. Les entreprises clientes l'utilisent pour leurs propres équipes, et souvent pour le compte de leurs propres clients.

Hébergé en Allemagne
Serveurs et sauvegardes dans l'Union européenne, sur une infrastructure certifiée ISO/IEC 27001.

IA française par défaut
Avec Mistral AI, aucune donnée de prospect ne quitte l'Union européenne.

Données cloisonnées
Chaque entreprise ne voit que ses données. Le cloisonnement est imposé par le serveur.

Le client garde la main
Une boîte mail connectée se retire en un clic, depuis BULLS CRM ou depuis Microsoft et Google.

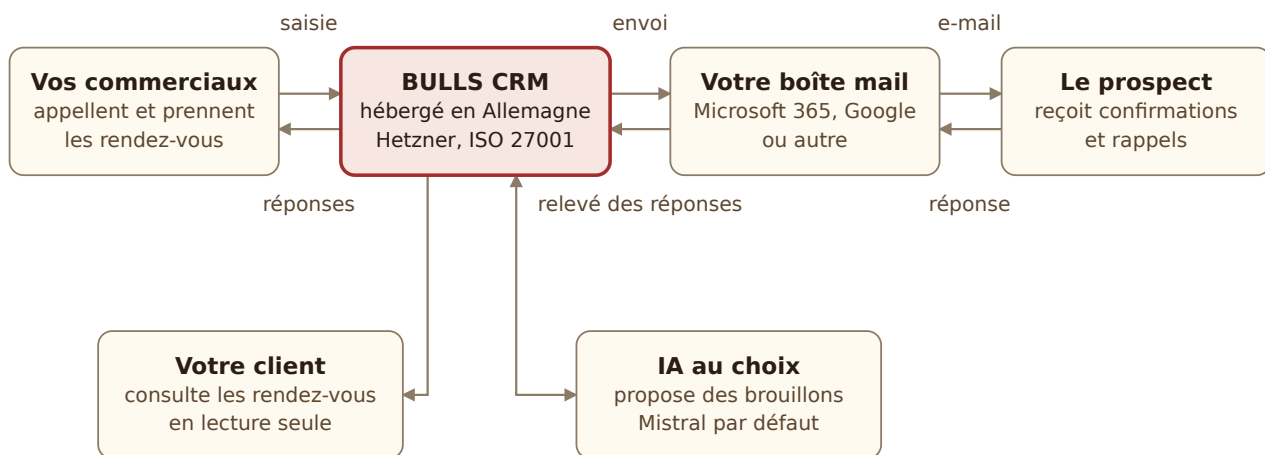
Qui est responsable de quoi

Acteur	Rôle RGPD	Ce qu'il fait
L'entreprise cliente	Responsable du traitement (ou sous-traitant de son propre client)	Décide de la prospection, des données importées et des messages envoyés
Bullaria, éditeur de BULLS CRM	Sous-traitant (article 28)	Fournit le logiciel, l'hébergement et l'envoi des e-mails

- **Éditeur** : Bullaria (Steve Taupenot-Bullara, entrepreneur individuel, nom commercial Bulls Sales, Lisbonne, NIF 302518614). Contact : steve@bullaria.com.
- **Accord de sous-traitance** : en annexe des conditions d'utilisation de Bullaria. Un modèle d'accord est aussi fourni pour que l'entreprise cliente le signe avec son propre client.
- **Usage des données** : aucune donnée n'est vendue, cédée ou utilisée à d'autres fins que le service.

Le parcours des données

Les e-mails passent par votre boîte, le CRM ne garde que les réponses



Les mails automatiques partent uniquement à partir des modèles de l'entreprise. L'IA ne fait que proposer des brouillons de relance : rien ne part sans qu'un commercial relise et clique sur « Envoyer ».

Connexion d'une boîte mail

BULLS CRM envoie les e-mails depuis la boîte de l'entreprise : Microsoft 365, Google ou toute boîte classique. L'accès porte uniquement sur la boîte connectée.

Fournisseur	Droits demandés	À quoi ils servent
Microsoft 365	User.Read, Mail.Send, Mail.Read, offline_access	Connaître l'adresse, envoyer les e-mails, ranger les réponses des prospects, garder la connexion active
Google	gmail.send, gmail.readonly	Envoyer les e-mails, ranger les réponses des prospects
Autre boîte	Adresse et mot de passe de la boîte	Envoi et réception classiques

- Seuls les nouveaux e-mails, arrivés après la connexion, sont relevés. L'historique n'est jamais importé.
- Seules les réponses des prospects suivis dans le CRM sont conservées. Les autres e-mails sont ignorés et jamais stockés.
- Aucun accès aux fichiers, agendas, contacts ou autres boîtes de l'entreprise.
- Avec Microsoft et Google, BULLS CRM ne voit jamais le mot de passe. Les jetons d'accès et les mots de passe de boîte sont stockés chiffrés (AES-256-GCM).
- Retrait à tout moment : bouton « Supprimer la boîte » dans BULLS CRM, ou suppression de l'application dans l'administration Microsoft ou Google.

Hébergement

Brique	Fournisseur	Lieu	Certification
Serveur, base de données, fichiers	Hetzner Online GmbH	Allemagne (UE)	ISO/IEC 27001:2022
Sauvegardes chiffrées	Hetzner Storage Box	Allemagne (UE)	ISO/IEC 27001:2022

Un accord de sous-traitance (article 28 RGPD) est signé avec Hetzner. Hetzner est audité chaque année par TÜV Rheinland.

Mesures de sécurité

Domaine	Mesure
Cloisonnement	Chaque donnée porte l'identifiant de son entreprise. Le filtre est imposé par le serveur : une entreprise ne peut pas lire les données d'une autre.
Accès	Compte nominatif pour chaque utilisateur, sessions signées qui expirent après 12 heures, droits selon le rôle.
Mots de passe	Jamais stockés en clair (empreinte scrypt avec sel). Liens de réinitialisation à usage unique, valables 30 minutes.
Traçabilité	Journal d'accès : qui a consulté quoi, et quand.
Chiffrement	Toutes les connexions en HTTPS. Sauvegardes, jetons et mots de passe de boîte chiffrés.
Réseau	Pare-feu fermé par défaut. Base de données et services internes non joignables depuis Internet.
Administration	Accès administrateur réservé à l'éditeur, par clé cryptographique uniquement, blocage automatique des tentatives répétées.
Mises à jour	Mises à jour de sécurité du système appliquées automatiquement chaque jour.
Sauvegardes	Chaque nuit, chiffrées, hors du serveur principal. Gardées 7 jours, 4 semaines et 6 mois. Restauration testée.
Surveillance	Contrôle automatique de la disponibilité avec alerte, audit technique chaque jour ouvré.
Incidents	Toute violation de données est signalée au client sans délai, au plus tard 48 heures après sa découverte.

Correspondance avec la norme ISO 27001

Nos mesures, rapportées aux thèmes de l'annexe A de la norme ISO/IEC 27001:2022.

Thème (annexe A)	Ce que nous faisons	État
Rôles et responsabilités (5.2)	Un responsable de la sécurité : l'éditeur.	En place
Fournisseurs (5.19 à 5.22)	Hébergeur certifié ISO 27001, accord RGPD signé, liste des sous-traitants publiée.	En place
Gestion des incidents (5.24 à 5.28)	Détection, coupure de l'accès, information du client sous 48 heures, compte rendu.	En place
Continuité (5.29, 5.30)	Sauvegards quotidiennes et restauration testée.	En partie
Données personnelles (5.34)	Accords de sous-traitance, aide aux demandes des personnes.	En place
Sécurité physique (7.1 à 7.14)	Centres de données Hetzner certifiés.	Hébergeur
Contrôle d'accès (8.2 à 8.5)	Comptes nominatifs, rôles, sessions limitées, administration par clé.	En place
Chiffrement (8.24)	En transit, sauvegards, jetons et mots de passe de boîte.	En partie
Mises à jour (8.8)	Correctifs de sécurité appliqués automatiquement.	En place
Sauvegards (8.13)	Chaque nuit, chiffrées, hors du serveur, contrôle d'intégrité hebdomadaire.	En place
Journalisation et surveillance (8.15, 8.16)	Journal d'accès, contrôle de disponibilité, audit quotidien.	En place
Sécurité du réseau (8.20 à 8.22)	Pare-feu, services internes non exposés, cloisonnement entre clients.	En place

Sous-traitants

Prestataire	Rôle	Lieu
Hetzner Online GmbH	Hébergement et sauvegards	Allemagne (UE)
Mistral AI	IA par défaut (relances, assistant, rapports)	France, hébergement UE
Anthropic, OpenAI	IA au choix de l'entreprise	États-Unis, clauses contractuelles types UE
Google	Connexion par compte Google (facultative), e-mails de mot de passe	UE / États-Unis
Stripe	Paiement des abonnements	Irlande / États-Unis

- L'entreprise choisit son IA dans BULLS CRM. Les données transmises ne servent pas à entraîner les modèles, et seul le texte utile est transmis.
- Tout nouveau sous-traitant est annoncé 30 jours à l'avance, avec droit d'opposition.

Droits des personnes et fin de contrat

Sujet	Engagement
Demandes des personnes	Accès, rectification, effacement, opposition : exécutés sur demande du client.
Opposition	Un prospect qui refuse est exclu des appels et des e-mails.
Fin de contrat	Export des données sur demande, puis suppression sous 30 jours.
Sauvegardes	Les données supprimées disparaissent des sauvegardes sous 6 mois, par rotation.
Audit	Informations fournies sur demande ; audit possible une fois par an, avec 30 jours de préavis.

Limites connues

- Le disque du serveur n'est pas chiffré ; les sauvegardes, jetons et mots de passe de boîte le sont.
- Pas d'engagement de disponibilité chiffré : le service tourne sur un serveur principal, restaurable à partir des sauvegardes.
- Sécurité contrôlée par des audits internes réguliers, pas encore par un cabinet indépendant.

Documents de référence : conditions d'utilisation (bullaria.com/univers/conditions-utilisation.html), politique de confidentialité (bullaria.com/univers/mentions-legales.html), certification Hetzner (hetzner.com/unternehmen/zertifizierung). Contact : steve@bullaria.com.