

Mesures Techniques et Organisationnelles (TOMs)

Version 1.0 — En vigueur au 5 juin 2026

Annexe sécurité au titre de l'article 32 du RGPD (sécurité du traitement). Ce document décrit les mesures **réellement en place** pour protéger les données traitées par Maestor. Les éléments encore en construction sont explicitement marqués « cible ».

1. Hébergement et souveraineté

- Serveur **dédié et isolé** sur Infomaniak Public Cloud (OpenStack), **datacenter de Genève (Suisse)** — ressources non partagées.
- Données hébergées **exclusivement en Suisse** (nLPD ; décision d'adéquation UE-Suisse).
- Hébergeur certifié **ISO 27001:2022** et ISO 50001, 100 % énergies renouvelables.
- Aucune télémétrie applicative envoyée à un service tiers : la supervision est **auto-hébergée**.

2. Chiffrement

Couche	Mesure
En transit	TLS 1.3 / 1.2 uniquement, Perfect Forward Secrecy (ECDHE/AES-GCM), HSTS, redirection HTTPS systématique, certificats automatisés.
Au repos	Base de données MariaDB chiffrée et volume de stockage chiffré — les données sur disque sont illisibles sans les clés.
Temps réel	Canal WebSocket chiffré (wss), canaux privés signés et cloisonnés.

3. Contrôle d'accès et authentification

- **Double authentification** : code temporaire (TOTP, application d'authentification) pour les accès d'administration ; code à usage unique par e-mail pour les utilisateurs (sans application à installer).
- **Contrôle d'accès basé sur les rôles (RBAC)** granulaire : permissions par module et par action, personnalisables par organisation et par rôle, jusqu'au niveau utilisateur.
- **Masquage des champs sensibles** (marge, prix d'achat, chiffre d'affaires) selon les droits, appliqué côté serveur.
- Accès administrateur système par **clé cryptographique uniquement** ; mot de passe et connexion root désactivés.
- **Limitation de débit** (rate-limiting) sur l'authentification contre les attaques par force brute.

4. Cloisonnement des données

- **Isolation multi-tenant** : chaque organisation et chaque réseau n'accède qu'à ses propres données.

- Pas de remontée centralisée des données des réseaux/grands comptes (engagement de confidentialité).
- Séparation stricte des environnements de **développement et de production**.

5. Protection applicative

- Protections **CSRF**, en-têtes **CSP** (Content Security Policy) et **SRI** (Subresource Integrity).
- Secrets applicatifs stockés hors de la racine web, permissions restreintes au service.
- **Journal d'audit** horodaté des actions sensibles.
- Détection et bannissement automatique des intrusions (**fail2ban**).
- Runtime maintenu à jour : PHP 8.3, mises à jour de sécurité automatiques.

6. Sauvegarde et continuité

- **Sauvegardes chiffrées quotidiennes** externalisées hors-serveur chez un dépositaire suisse (chiffrement de bout en bout).
- **Restauration testée**.
- Objectifs de continuité : **RPO 24 h / RTO 4 h**.
- Voir la *Politique de sauvegarde & de continuité d'activité* pour le détail.

7. Supervision

- **Uptime externe** : sondes indépendantes toutes les 60 s sur les services publics (contrôle du contenu, pas seulement du code HTTP).
- **Infrastructure** : métriques temps réel (CPU, mémoire, disque, réseau, base de données, services).
- **Erreurs applicatives** : remontée et historisation **auto-hébergées et souveraines**.

8. Protection des données personnelles (RGPD)

- **Purge RGPD** automatisée selon les durées de conservation.
- **Signature électronique eIDAS** (Yousign) pour les documents engageants.
- **Scellement par empreinte SHA-256** des exports à valeur juridique.
- Registre des sous-traitants ultérieurs maintenu à jour : <https://trust.maestor.eu/sous-traitants>
- DPA conforme à l'article 28 disponible : <https://trust.maestor.eu/documents>

9. Mesures organisationnelles

- NDA signés, sensibilisation sécurité, processus d'arrivée/départ documenté.
- Déploiements tracés ; revue de code et revue de sécurité avant tout déploiement sensible (authentification, accès, facturation).
- Gestion des incidents documentée (voir la *Politique de gestion des incidents*).

Référence complète et à jour des mesures : <https://trust.maestor.eu/securite>