

Accord de Sous-Traitance des Données (DPA)

Version 1.1 — En vigueur au 5 juin 2026

Conforme à l'article 28 du RGPD (Règlement (UE) 2016/679)

1. Parties

Responsable du traitement (le « Client ») : entité ayant souscrit aux Services Maestor, désignée dans le Bon de Commande ou le Contrat Cadre.

Sous-traitant (« Maestor ») : entité juridique opérant les Services Maestor — voir Mentions légales sur <https://maestor.eu/mentions-legales>.

Ensemble désignées les « Parties ».

2. Définitions

Les termes en majuscules ont le sens qui leur est attribué dans le RGPD. Sans préjudice de cette définition générale :

- « **Données** » : les Données à caractère personnel traitées par Maestor pour le compte du Client dans le cadre des Services.
- « **Services** » : les Services Maestor souscrits par le Client (CRM, SAV, app poseur, IA conversationnelle, etc.).
- « **Sous-traitant ultérieur** » : tout tiers à qui Maestor a recours pour réaliser tout ou partie des Services.
- « **Violation** » : violation de la sécurité au sens de l'article 4(12) du RGPD.

3. Objet, nature et finalité du traitement

Élément	Détail
Objet du traitement	Exécution des Services Maestor souscrits par le Client
Nature du traitement	Collecte, enregistrement, structuration, conservation, consultation, communication, effacement, destruction
Finalités	Pilotage métier (CRM, devis, SAV, pose, facturation, communication client)
Durée du traitement	Durée du Contrat + durées légales de conservation (cf. § 11)

4. Catégories de Données et de personnes concernées

Données traitées

- **Identification** : nom, prénom, raison sociale, adresse postale, email, téléphone.
- **Données contractuelles** : commandes, devis, contrats, factures, paiements.
- **Données de pose et SAV** : photos chantier, descriptifs technique, signatures électroniques.
- **Données de communication** : transcriptions d'appels (Sophie IA, si activé), historiques de chat (Sofia IA, si activé), emails et SMS.
- **Données de connexion** : adresses IP, logs d'accès, identifiants utilisateurs.
- **Données de paiement** : tokens Stripe uniquement (PAN jamais stocké chez Maestor).

Personnes concernées

- Clients finaux du Client (particuliers, professionnels).
 - Collaborateurs du Client (utilisateurs des Services).
 - Prospects et contacts commerciaux du Client.
-

5. Obligations et droits du Client (Responsable)

Le Client :

1. Détermine les finalités et moyens du traitement.
 2. S'assure de la licéité du traitement (base légale RGPD adaptée).
 3. Recueille les consentements lorsque requis.
 4. Informe les personnes concernées conformément aux articles 13 et 14 du RGPD.
 5. Gère les demandes d'exercice des droits (accès, rectification, effacement, opposition, portabilité, limitation).
 6. Notifie aux autorités les Violations dont il est responsable.
-

6. Obligations de Maestor (Sous-traitant)

Maestor s'engage à :

1. **Ne traiter les Données que sur instruction documentée** du Client (le Contrat valant instruction).
2. **Confidentialité** : garantir que les personnes autorisées à traiter les Données sont soumises à une obligation de confidentialité contractuelle ou légale.
3. **Sécurité** (article 32 RGPD) : mettre en œuvre les mesures techniques et organisationnelles appropriées (voir Annexe 1).
4. **Sous-traitance ultérieure** : informer le Client de tout recours à des sous-traitants ultérieurs (voir Annexe 2) et permettre l'objection.
5. **Assistance** au Client pour répondre aux demandes d'exercice des droits.
6. **Assistance** au Client dans l'évaluation d'impact (AIPD/DPIA) et la consultation préalable de l'autorité (articles 35 et 36 RGPD).

7. **Notification des Violations** : notifier sans délai injustifié au Client, et en tout état de cause sous 48 heures après en avoir pris connaissance.
 8. **Suppression / Restitution** : à l'issue du Contrat, restituer ou détruire les Données selon l'instruction du Client.
 9. **Documentation** : tenir à disposition les informations nécessaires pour démontrer le respect du présent DPA.
 10. **Audit** : se soumettre aux audits du Client (voir § 12).
-

7. Localisation et transferts hors UE

Hébergement principal

Les Données sont hébergées **en Suisse** chez **Infomaniak Network SA** (Genève / Lausanne), datacenters certifiés ISO 27001:2022 et ISO 14001, refroidis à l'eau de Genève, énergies hydroélectriques.

La Suisse bénéficie d'une **décision d'adéquation** de la Commission européenne (décision 2000/518/CE confirmée).

Sous-traitants ultérieurs avec transfert hors UE

Certains traitements impliquent des sous-traitants soumis au droit américain (Anthropic — IA Claude, Twilio — SMS/vocal, ElevenLabs — synthèse vocale). Ces transferts sont encadrés par :

- Les **Clauses Contractuelles Types** (CCT, décision (UE) 2021/914) signées avec chaque fournisseur.
- Une **analyse de transfert** (TIA) documentant les garanties supplémentaires.
- Une **purge automatique** des Données chez les sous-traitants IA (rétention < 30 jours).

Le Client est informé que les autorités américaines peuvent, en application du **CLOUD Act** et de la **section 702 du FISA**, demander l'accès aux Données traitées par ces sous-traitants américains. Maestor minimise ces transferts et privilégie en permanence des alternatives européennes lorsqu'elles deviennent matures.

8. Sous-traitants ultérieurs

Le Client autorise Maestor à recourir aux sous-traitants ultérieurs listés en **Annexe 2**.

Toute modification de cette liste sera notifiée au Client au moins **30 jours avant** sa mise en œuvre. Le Client dispose d'un droit d'objection motivé.

9. Sécurité

Les mesures techniques et organisationnelles mises en place par Maestor sont décrites :

- En **Annexe 1** du présent DPA (vue synthétique).
- En détail sur le **Trust Center** : <https://trust.maestor.eu>

Mesures principales : chiffrement TLS 1.3 (transit), AES-256 (repos), RBAC, audit logs, sauvegardes quotidiennes, hash bcrypt, principe de moindre privilège, séparation des environnements, tests de sécurité.

10. Notification de Violation

En cas de Violation affectant les Données du Client :

1. **Délai** : notification sous **48 heures** maximum après la prise de connaissance.
2. **Canal** : email au DPO du Client (ou au contact privilégié déclaré) + duplication par lettre recommandée si > P1.
3. **Contenu** : nature de la Violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées.
4. **Coopération** : assistance au Client pour la notification à la CNIL (article 33 RGPD) et aux personnes concernées (article 34 RGPD) si requis.

11. Conservation et destruction des Données

Catégorie de Données	Durée de conservation active	Archivage légal
Compte utilisateur	Durée du Contrat	5 ans après cessation
Dossiers SAV	5 ans après clôture	+ 5 ans archivage
Factures	10 ans (obligation légale)	—
Transcriptions IA (Sophie)	12 mois	—
Photos chantier	36 mois après clôture	—
Logs techniques	6 mois	—

À l'issue du Contrat, à la demande écrite du Client, Maestor procède à la **destruction sécurisée** des Données (suppression logique et physique) ou à leur **restitution** au format CSV/JSON dans un délai de **30 jours**.

12. Audit

Le Client (ou un tiers indépendant mandaté par lui, sous accord de confidentialité) peut auditer la conformité de Maestor au présent DPA :

- Préavis : **30 jours**.
- Fréquence : au maximum **une fois par an**, sauf incident.
- Périmètre : politique de sécurité, mesures techniques, registres de sous-traitance, journaux d'audit (sans accès aux Données d'autres clients).
- Frais : à la charge du Client, sauf si l'audit révèle un manquement substantiel imputable à Maestor.

Pour limiter les audits redondants, Maestor met à disposition sur <https://trust.maestor.eu> :

- Le Trust Center à jour (mesures techniques, sous-traitants, certifications).
- Les rapports d'audit externes (à compter de la certification ISO 27001 prévue Q3 2028).
- Le registre des incidents publics.

13. Responsabilité et indemnisation

Les obligations et responsabilités des Parties sont définies dans le Contrat Cadre. En cas de manquement aux obligations RGPD imputable à Maestor, ce dernier indemnise le Client des sommes qu'il aurait à reverser aux personnes concernées ou aux autorités, dans la limite et selon les modalités du Contrat.

14. Durée et survie

Le présent DPA prend effet à la date de signature du Contrat et reste en vigueur tant que Maestor traite des Données pour le compte du Client.

Les obligations de confidentialité et de notification de Violation **survivent** à la cessation du Contrat pendant **5 ans**.

15. Droit applicable et juridiction

Le présent DPA est régi par le droit français. Tout litige relèvera des juridictions compétentes désignées dans le Contrat Cadre.

Annexe 1 — Mesures techniques et organisationnelles (synthèse)

Domaine	Mesures
Chiffrement	TLS 1.3 obligatoire (transit), AES-256 (repos), HSTS preload
Authentification	MFA obligatoire pour les comptes admin, bcrypt pour les mots de passe, sessions expirantes
Contrôle d'accès	RBAC granulaire, principe de moindre privilège, séparation des rôles
Sauvegardes	Quotidiennes, hors-site Infomaniak, rétention 30 jours, restauration testée
Journalisation	Audit logs immuables sur toute action sensible, conservation 6 mois
Surveillance	Détection d'anomalies, alertes temps réel, astreinte 24/7 sur les incidents P0
Tests sécurité	Revue code sur PR sensible, Dependabot actif, pentest annuel planifié
Continuité	Sauvegardes quotidiennes, PCA/PRA documenté, RTO 4h, RPO 24h
Données IA	Purge auto < 30 jours chez sous-traitants IA, anonymisation des logs
Personnel	NDA signés, sensibilisation sécurité, processus offboarding documenté

Référence complète : <https://trust.maestor.eu/securite>

Annexe 2 — Sous-traitants ultérieurs (au 5 juin 2026)

Sous-traitant	Pays	Rôle	Catégories de Données	Garanties
Infomaniak Network SA	Suisse	Hébergement infrastructure, email transactionnel (SMTP), sauvegardes off-site	Toutes (chiffrées au repos)	ISO 27001, DPA signé, décision d'adéquation UE-CH
Stripe Payments Europe Ltd	Irlande	Traitement paiements	Tokens carte, identité payeur	PCI-DSS Level 1, RGPD compliant
Anthropic, PBC	États-Unis	IA Claude (Sofia chat, Sophie IA)	Transcriptions, prompts	CCT + TIA, purge < 30 jours
Twilio Inc.	États-Unis	Téléphonie / SMS / WhatsApp	Numéros, transcriptions vocales	CCT + TIA, isolation environnement EU
ElevenLabs Inc.	États-Unis	Synthèse vocale IA	Voix synthétiques, scripts	CCT + TIA, pas de Données identifiantes envoyées
Yousign SAS	France	Signature électronique eIDAS	Identité signataires, documents	eIDAS niveau avancé/qualifié, ISO 27001
MapTiler AG	Suisse	Géocodage inversé (watermark photos terrain)	Coordonnées GPS (pas d'identité)	Société suisse (nLPD), RGPD
INSEE — API Sirene	France	Consultation de données publiques d'entreprise (SIREN/SIRET)	N° SIREN/SIRET (données publiques)	Service public, Open Data, RGPD
monday.com Ltd.	États-Unis	Intégration CRM externe — optionnelle (activée par le Client)	Données synchronisées si activée	DPA, SOC 2, ISO 27001, CCT
Pipedrive OÜ	Estonie (UE)	Intégration CRM externe — optionnelle (activée par le Client)	Données synchronisées si activée	DPA, ISO 27001, éditeur UE

Mise à jour temps réel : <https://trust.maestor.eu/sous-traitants>

Signatures

Pour le Client : _____

Nom et fonction :

Date :

Pour Maestor : _____

Nom et fonction :

Date :

Document généré depuis le template Maestor DPA v1.1. La version officielle signée prévaut. Pour toute question : dpo@maestor.eu

Maestor — Document de conformité. La version officielle signée prévaut. Contact : security@maestor.eu / dpo@maestor.eu