Annexe 1. Accord de traitement des données (contrat de sous-traitance)

Version 2.0 · 8 novembre 2026

Ceci est une traduction. En cas de divergence, le texte néerlandais prévaut.

SOMMAIRE

Article 1. Objet
Article 2. Instructions
Article 3. Confidentialité
Article 4. Sécurité
Article 5. Sous-traitants ultérieurs
Article 6. Transfert en dehors de l'Espace économique européen
Article 7. Droits des personnes concernées
Article 8. Violations de données à caractère personnel
Article 9. Assistance et contrôle
Article 10. Fin du traitement
Article 11. Responsabilité et durée
Annexe A. Description des traitements
Annexe B. Sous-traitants ultérieurs
Annexe C. Mesures de sécurité

Le présent accord de traitement des données fait partie des conditions générales de mBino Services et s'applique lorsque mBino Services (**Sous-traitant**), dans le cadre de la fourniture des Services, traite des données à caractère personnel pour le compte du Client (**Responsable du traitement**). Les notions du Règlement général sur la protection des données (RGPD), telles que données à caractère personnel, traitement, personne concernée et violation de données à caractère personnel, ont le sens que leur donne le RGPD. Les autres termes commençant par une majuscule ont le sens que leur donnent les conditions générales.

Article 1. Objet

1.1. Le Sous-traitant ne traite des données à caractère personnel que dans la mesure nécessaire à la fourniture des Services, tels que décrits dans le Contrat et à l'annexe A.

1.2. Le Client détermine la finalité et les moyens du traitement. Le Client garantit que le traitement est licite, qu'il dispose d'une base juridique et qu'il informe les personnes concernées, telles que ses clients d’hôtel, clients, visiteurs et collaborateurs.

Article 2. Instructions

2.1. Le Sous-traitant ne traite les données à caractère personnel que sur la base des instructions données Par écrit par le Client. Le Contrat, le présent accord de traitement des données et les paramètres que le Client choisit dans les Services valent instructions.

2.2. Le Sous-traitant peut traiter des données à caractère personnel si une obligation légale l'exige. Il en informe le Client au préalable, sauf si la loi l'interdit.

2.3. Si le Sous-traitant estime qu'une instruction enfreint le RGPD ou d'autres règles relatives à la protection des données, il en informe immédiatement le Client.

Article 3. Confidentialité

3.1. Le Sous-traitant veille à ce que les personnes qui traitent les données à caractère personnel soient tenues au secret, et à ce que seules les personnes qui en ont besoin pour leur travail y aient accès.

Article 4. Sécurité

4.1. Le Sous-traitant prend des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la perte et tout traitement illicite, compte tenu de l'état de la technique, des coûts, ainsi que de la nature et des risques du traitement. L'annexe C décrit les principales mesures.

4.2. Le Sous-traitant peut adapter les mesures, pour autant que le niveau de sécurité ne diminue pas.

Article 5. Sous-traitants ultérieurs

5.1. Le Client donne au Sous-traitant une autorisation générale de faire appel à des sous-traitants ultérieurs. Les sous-traitants ultérieurs au moment de la signature figurent à l'annexe B.

5.2. Le Sous-traitant informe le Client au moins trente jours à l'avance, par e-mail, dans le Compte ou sur le Site web, de tout nouveau sous-traitant ultérieur ou de tout remplacement. Le Client peut formuler une objection motivée dans ce délai. Si les parties ne parviennent pas à trouver une solution, le Client peut résilier le Service concerné à la date à laquelle il est fait appel au sous-traitant ultérieur.

5.3. Le Sous-traitant impose aux sous-traitants ultérieurs les mêmes obligations que celles prévues dans le présent accord de traitement des données, et reste responsable envers le Client de leur respect.

5.4. Les parties avec lesquelles le Client a lui-même conclu un contrat et dont il active l'intégration dans les Services, telles que son prestataire de services de paiement, son channel manager, son logiciel comptable ou son système de caisse, ne sont pas des sous-traitants ultérieurs du Sous-traitant. Le Client est lui-même responsable de la transmission des données à ces parties.

Article 6. Transfert en dehors de l'Espace économique européen

6.1. Le Sous-traitant traite les données à caractère personnel autant que possible au sein de l'Espace économique européen (EEE). Un transfert en dehors de celui-ci n'a lieu que si un niveau de protection adéquat est garanti, par exemple au moyen d'une décision d'adéquation (dont le cadre de protection des données UE-États-Unis) ou des clauses contractuelles types de la Commission européenne. L'annexe B mentionne les sous-traitants ultérieurs situés en dehors de l'EEE.

Article 7. Droits des personnes concernées

7.1. Les Services offrent des fonctions permettant de traiter les demandes des personnes concernées, telles que l'accès, l'exportation et l'anonymisation des profils de clients d'hôtel. Si le Client ne peut pas traiter lui-même une demande à l'aide de ces fonctions, le Sous-traitant l'aide dans des limites raisonnables.

7.2. Si le Sous-traitant reçoit lui-même une demande d'une personne concernée, il la transmet au Client dans les plus brefs délais et n'y répond pas lui-même sur le fond, sauf si le Client le lui demande.

Article 8. Violations de données à caractère personnel

8.1. Le Sous-traitant notifie au Client toute violation de données à caractère personnel concernant les données à caractère personnel du Client, dans les meilleurs délais et si possible dans les 48 heures après en avoir pris connaissance.

8.2. Le Sous-traitant fournit à cette occasion les informations dont il dispose, et les complète dès qu'il en sait davantage : la nature de la violation, les catégories concernées et le nombre approximatif de personnes concernées et de données, les conséquences probables et les mesures prises ou proposées.

8.3. Le Client décide s'il notifie la violation à l'autorité de contrôle et aux personnes concernées. Le Sous-traitant l'aide à cet égard.

Article 9. Assistance et contrôle

9.1. Le Sous-traitant aide le Client, dans des limites raisonnables, dans le cadre d'une analyse d'impact relative à la protection des données (AIPD) et d'une consultation préalable de l'autorité de contrôle, dans la mesure où celles-ci concernent les Services.

9.2. Le Sous-traitant fournit au Client les informations nécessaires pour démontrer le respect des obligations découlant du présent accord de traitement des données. Le Client peut, à ses frais et au maximum une fois par an, faire réaliser un audit par un expert indépendant tenu au secret, moyennant un préavis d'au moins quatorze jours, sans perturber de manière déraisonnable les activités du Sous-traitant. Le Sous-traitant peut, à la place, fournir un rapport d'audit récent ou un certificat émanant d'une partie indépendante.

9.3. L'assistance fournie en vertu du présent article et de l'article 7 qui exige plus qu'un effort limité peut être facturée par le Sous-traitant à ses tarifs habituels, sauf si l'assistance est rendue nécessaire par un manquement du Sous-traitant.

Article 10. Fin du traitement

10.1. Après la fin du Contrat, le Sous-traitant met les données à caractère personnel à disposition sur demande, puis les supprime, comme prévu à l'article 16 des conditions générales. Les données à caractère personnel soumises à une obligation légale de conservation sont conservées par lui aussi longtemps que dure cette obligation, et il ne les utilise à aucune autre fin pendant cette période.

Article 11. Responsabilité et durée

11.1. La responsabilité du Sous-traitant est régie par l'article 11 des conditions générales.

11.2. Le présent accord de traitement des données s'applique aussi longtemps que le Sous-traitant traite des données à caractère personnel pour le Client. Les dispositions qui, de par leur nature, sont destinées à rester en vigueur par la suite restent d'application.

11.3. Si les parties ont signé un accord de traitement des données distinct, celui-ci prévaut sur la présente annexe.

Annexe A. Description des traitements

Service	Personnes concernées	Données à caractère personnel	Finalité
KEOR PMS et les applications KEOR PMS Staff, KEOR Guest et KEOR Display	Clients d'hôtel, personnes de contact d'entreprises et d'organisateurs, collaborateurs du Client	Nom, coordonnées, adresse, date de naissance, nationalité, données et photo de la pièce d'identité (si le Client active cette fonction), données de séjour et de réservation, préférences et notes, signatures, factures et paiements (pas de numéros de carte complets), demandes et messages ; pour les collaborateurs : nom, e-mail, rôle, identifiants de connexion, utilisation et modifications dans les journaux, jetons push	Réservations, check-in et check-out, facturation, housekeeping et maintenance, événements et groupes, communication avec les clients d'hôtel, reporting et enregistrements légaux

Service	Personnes concernées	Données à caractère personnel	Finalité
KEOR POS	Collaborateurs, clients du Client et clients d'hôtel	Pour les collaborateurs : nom, langue, droits, code PIN (haché), heures de pointage et, en cas de système de caisse enregistreuse, le numéro de registre national (chiffré) ; ventes ; fichier clients (nom, entreprise, coordonnées, numéro de TVA, notes) ; données des clients de l'hôtel via KEOR PMS (nom, chambre, séjour, signature ; photos uniquement affichées, non conservées)	Caisse, commandes, paiements, gestion des clients, imputations sur la chambre et enregistrement légal de caisse
Hébergement et e-mail	Clients du Client, visiteurs de son site web, expéditeurs et destinataires d'e-mails	Toutes les données que le Client stocke sur son site web, dans ses bases de données et ses boîtes aux lettres électroniques, ainsi que les fichiers journaux	Stockage et disponibilité
Réseaux Wi-Fi et portails invités	Utilisateurs du réseau du Client	Adresse e-mail ou numéro de téléphone lors de la connexion, identifiant de l'appareil (adresse MAC), adresse IP, données de session et, en cas de services de localisation, la position des appareils	Accès au réseau, gestion, sécurité et (si le Client les active) services de localisation
Téléphonie	Collaborateurs du Client et leurs interlocuteurs	Numéros de téléphone, noms, données d'appel (qui, quand, combien de temps), messagerie vocale, enregistrements d'appels (si le Client les active), messages via des canaux connectés	Téléphonie, transfert d'appels, reporting et (si le Client les active) enregistrements
Gestion informatique, sauvegarde et assistance à distance	Collaborateurs du Client et toute personne dont des données figurent dans ses systèmes	Toutes les données figurant dans les systèmes, boîtes aux lettres électroniques et sauvegardes que le Sous-traitant gère, ainsi que les fichiers journaux des sessions à distance	Gestion, maintenance, sauvegarde, restauration et assistance

Service	Personnes concernées	Données à caractère personnel	Finalité
Développement de sites web et de logiciels	Comme ci-dessus, dans la mesure où le Sous-traitant a accès aux données de production	Données figurant dans les systèmes du Client	Développement, tests et livraison

Le traitement dure aussi longtemps que le Contrat est en cours, puis aussi longtemps que nécessaire conformément à l'article 10.

Annexe B. Sous-traitants ultérieurs

Sous-traitant ultérieur	Lieu du traitement	Objet	Pour quels Services
Contabo GmbH	Allemagne	Hébergement des serveurs et des bases de données du Sous-traitant, avec leurs sauvegardes	KEOR, hébergement, assistance à distance, et serveurs de réseau et de téléphonie que le Sous-traitant héberge lui-même
Cloudflare, Inc.	Réseau mondial ; entreprise établie aux États-Unis (cadre de protection des données UE-États-Unis et clauses contractuelles types)	Sécurité et transmission du trafic web (proxy, DNS)	KEOR, sites web
Google LLC (Firebase Cloud Messaging)	États-Unis (cadre de protection des données UE-États-Unis et clauses contractuelles types)	Envoi de notifications push aux applications ; textes de notification courts et jetons d'appareil	KEOR PMS Staff, KEOR Guest
Apple Inc. (Apple Push Notification service)	États-Unis (cadre de protection des données UE-États-Unis et clauses contractuelles types)	Envoi de notifications push sur iPhone et iPad	KEOR PMS Staff, KEOR Guest
Recommand	Belgique	Point d'accès Peppol pour l'envoi et la réception de factures électroniques	KEOR (uniquement si le Client facture via Peppol)

Sous-traitant ultérieur	Lieu du traitement	Objet	Pour quels Services
Module2	Belgique	Signature des données fiscales par le module fiscal (FDM)	KEOR POS (uniquement en cas de système de caisse enregistreuse)

La gestion des réseaux Wi-Fi (RUCKUS Virtual SmartZone), des centraux téléphoniques (Yeastar P-Series) et de l'assistance à distance (ScreenConnect) fonctionne sur des serveurs que le Sous-traitant héberge lui-même, ou chez le Client. Les fournisseurs de ces logiciels ne sont donc pas des sous-traitants ultérieurs.

Ne figurent pas dans cette liste les parties avec lesquelles le Client a lui-même conclu un contrat et dont il active l'intégration (article 5.4), telles que Viva (paiements), Channex ou Cubilis (channel manager), Clearfacts (comptabilité), Lightspeed (caisse) et les sites de réservation. Les e-mails de KEOR passent par le serveur de messagerie propre du Sous-traitant, ou par le serveur de messagerie que le Client configure lui-même.

Annexe C. Mesures de sécurité

- Toutes les connexions aux Services sont chiffrées (HTTPS avec HSTS) ; le trafic web passe par Cloudflare.
- Les champs sensibles sont stockés sous forme chiffrée, tels que les numéros de document des clients d'hôtel, les secrets d'authentification à deux facteurs, les identifiants de connexion des intégrations, les clés des liens invités et les résultats des scans d'identité.
- Les mots de passe ne sont stockés que sous forme de hachage (bcrypt). Les tentatives de connexion sont limitées.
- L'authentification à deux facteurs (TOTP avec codes de récupération) est obligatoire pour les administrateurs de la plateforme et peut être rendue obligatoire par rôle par le Client.
- Droits par rôle. Les données des différents clients sont séparées dans le logiciel.
- Un journal d'audit enregistre les modifications, notamment l'anonymisation de clients d'hôtel et la réinitialisation de l'authentification à deux facteurs.
- Les numéros de carte complets et les codes de sécurité des cartes de paiement ne sont pas stockés.
- Les photos des pièces d'identité sont conservées selon le délai fixé par le Client, allant de l'absence de conservation jusqu'à la fin du séjour, puis supprimées automatiquement.
- Les bases de données ne sont pas directement accessibles depuis internet.
- Sauvegardes quotidiennes, avec une copie hors du serveur, au sein de l'UE. Les sauvegardes et les fichiers journaux sont conservés trente jours, sauf si la loi impose un délai plus long.

- L'assistance à distance passe par un serveur que le Sous-traitant héberge lui-même, avec des fichiers journaux de chaque session, conservés un an (365 jours). Les sessions ne sont enregistrées que si cela a été convenu avec le Client.
- Les collaborateurs et les personnes auxquelles il est fait appel sont tenus au secret.