Contrat de sous-traitance

Version 2026-11, valable à partir du 4 novembre 2026.

Parties

Le responsable du traitement : le cabinet qui s'inscrit dans Horalena, avec les données qu'il indique lors de l'inscription et dans Paramètres, ci-après « le Cabinet ». La personne qui accepte le contrat déclare être habilitée à engager le Cabinet. Si le Cabinet est un cabinet de groupe, un cercle ou un service hospitalier, cette personne accepte pour ce groupe et ses membres.

Le sous-traitant : Nena Consult BV, numéro d'entreprise 1010.714.363, Parkwijk 31, 9810 Nazareth-De Pinte, RPM Gand, division Gand, exploitant d'Horalena, ci-après « Nena Consult ».

Article 1. Objet et rôles

1.1 Nena Consult fournit au Cabinet le logiciel Horalena comme service en ligne. Ce faisant, Nena Consult traite des données à caractère personnel pour le compte du Cabinet. Pour ces données, le Cabinet est le responsable du traitement et Nena Consult le sous-traitant.

1.2 Ce contrat s'applique à toutes les données à caractère personnel que le Cabinet, ses utilisateurs, ses patients et les membres de ses rôles de garde encodent ou font traiter dans Horalena, comme décrit à l'annexe A.

1.3 Pour une série limitée de données, Nena Consult est elle-même responsable du traitement : les données du compte et des personnes de contact du Cabinet pour l'inscription, la facturation et la communication sur le service, l'avis donné par un utilisateur, les visites du site produit et les données de la démo publique. Ces traitements sortent du cadre de ce contrat et figurent dans la déclaration de confidentialité de Nena Consult.

Article 2. Instructions du Cabinet

2.1 Nena Consult traite les données uniquement sur instruction écrite du Cabinet. Ces instructions sont : ce contrat, les conditions d'utilisation, et ce que les utilisateurs du Cabinet paramètrent ou font dans Horalena.

2.2 Si Nena Consult est légalement tenue de traiter ou de communiquer malgré tout des données, elle le signale au préalable au Cabinet, sauf si la loi interdit ce signalement.

2.3 Si Nena Consult estime qu'une instruction enfreint le RGPD ou une autre règle sur la protection des données, elle le signale immédiatement au Cabinet.

2.4 Nena Consult n'utilise pas les données à ses propres fins, ne les vend pas et ne les transmet pas aux annuaires de soins qu'elle exploite. Elle peut toutefois en tirer des comptages sans données de patients (nombres par cabinet), uniquement pour gérer le service, facturer et reconnaître les abus.

Article 3. Confidentialité

3.1 Nena Consult ne donne accès aux données qu'aux personnes qui en ont besoin pour le service et qui sont tenues à une obligation de secret. Elle sait que les données peuvent relever du secret professionnel du prestataire de soins, et les traite en conséquence.

3.2 Aujourd'hui, il s'agit uniquement de l'administrateur de Nena Consult. Si du personnel ou un autre prestataire de services s'ajoute, cette liste est mise à jour et tenue à la disposition du Cabinet et de l'Autorité de protection des données.

3.3 Les écrans de gestion de Nena Consult n'affichent pas de données de patients. Nena Consult a toutefois un accès technique au serveur, à la base de données et aux clés. Elle n'utilise cet accès que si c'est nécessaire au fonctionnement du service ou à la demande du Cabinet. Si elle consulte à cette occasion des données d'un Cabinet, elle le signale ensuite aux administrateurs.

3.4 Nena Consult utilise pour le développement et la gestion des outils logiciels, y compris des assistants IA. Ceux-ci ne lisent pas de données de patients : sur le serveur, ils n'exécutent que des opérations techniques, comme déployer, vérifier des versions et compter. Si quelqu'un doit consulter de vraies données, l'administrateur le fait lui-même, sans ces outils.

Article 4. Sécurité

4.1 Nena Consult prend les mesures techniques et organisationnelles de l'annexe B.

4.2 Nena Consult peut adapter ces mesures si le niveau de protection ne baisse pas.

4.3 Le Cabinet est responsable de ce qui se passe de son côté : à qui il donne accès et avec quel rôle, le retrait à temps d'un compte, la sécurité de ses propres appareils, et ce qu'il fait d'un export.

4.4 Aucun test de sécurité indépendant n'a encore eu lieu et il n'y a pas de certification. L'annexe B indique ce qui existe et ce qui n'existe pas, afin que le Cabinet puisse juger lui-même si cela lui suffit.

Article 5. Sous-traitants ultérieurs

5.1 Le Cabinet donne à Nena Consult une autorisation générale de faire appel aux sous-traitants ultérieurs de l'annexe C.

5.2 Nena Consult signale un sous-traitant ultérieur nouveau ou remplaçant au moins 30 jours à l'avance par e-mail aux administrateurs du Cabinet. Le Cabinet peut formuler une objection motivée dans ce délai. Si les parties ne s'entendent pas, le Cabinet peut mettre fin à l'abonnement, avec remboursement de la partie non encore écoulée.

5.3 Nena Consult impose à chaque sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que dans ce contrat, et reste responsable de ce sous-traitant ultérieur envers le Cabinet.

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

6.1 Le serveur, la base de données et les sauvegardes se trouvent dans l'Union européenne. Nena Consult ne transfère pas les données en dehors de l'Espace économique européen, sauf sur instruction du Cabinet ou avec les garanties du chapitre V du RGPD.

6.2 Les e-mails d'Horalena passent par Google Workspace. Google est une entreprise américaine et peut aussi traiter ces messages en dehors de l'Espace économique européen. Pour cela, le règlement de sous-traitance de Google s'applique, avec les garanties du chapitre V du RGPD. Un tel e-mail ne contient jamais de diagnostic ni de rapport, mais bien le cabinet, le moment et le prestataire de soins (annexe C).

Article 7. Assistance pour les droits des personnes concernées

7.1 Le Cabinet répond lui-même aux questions des patients. Si Nena Consult reçoit une telle question, elle la transmet sans y répondre elle-même.

7.2 Horalena donne pour cela au Cabinet les moyens suivants : un export par patient, une copie complète pour le patient, un export de toutes les données du cabinet, une page « Qui a ouvert mon dossier ? », et la modification et le fait de barrer dans le dossier.

7.3 Ce que le Cabinet ne peut pas faire lui-même, comme effacer un patient qui n'a pas de dossier, Nena Consult le fait sur demande écrite dans les 10 jours ouvrables. Si une demande exige un travail inhabituel, une indemnité peut s'appliquer, après accord préalable.

Article 8. Assistance pour la sécurité, les fuites de données et l'AIPD

8.1 Si Nena Consult constate une violation de la sécurité des données, elle le signale sans retard injustifié et au plus tard dans les 48 heures par e-mail aux administrateurs du Cabinet, avec ce qui est connu à ce moment : la nature, les données et personnes concernées pour autant qu'elles soient connues, les conséquences et les

mesures prises.

8.2 Le Cabinet décide s'il prévient l'Autorité de protection des données et les personnes concernées (articles 33 et 34 du RGPD).

8.3 Nena Consult aide le Cabinet en fournissant des informations lors d'une analyse d'impact relative à la protection des données et d'une consultation préalable de l'Autorité de protection des données, et pour le respect des articles 32 à 36 du RGPD, compte tenu des informations dont elle dispose.

Article 9. Audit

9.1 Nena Consult fournit au Cabinet, sur demande, les informations nécessaires pour vérifier que ce contrat est respecté.

9.2 Le Cabinet peut, au maximum une fois par an et après un avis écrit d'au moins 30 jours, réaliser un audit ou le faire réaliser par un expert qu'il désigne et qui est tenu au secret. Un audit ne touche jamais aux données d'un autre cabinet. Les frais sont à charge du Cabinet.

9.3 En cas d'indication d'un manquement grave ou d'une question d'une autorité de contrôle, la limitation dans le temps ne s'applique pas.

Article 10. Durée et fin

10.1 Ce contrat s'applique aussi longtemps que Nena Consult traite des données pour le Cabinet.

10.2 Il ne peut être mis fin au contrat tant que des données du Cabinet se trouvent chez Nena Consult, sauf de la manière prévue à l'article 11.

Article 11. Données après la fin du service

11.1 Après la fin de l'abonnement, les données restent conservées et le Cabinet peut continuer à se connecter, à consulter et à exporter, sans frais, sauf si l'article 11.4 ou 11.5 s'applique. Nena Consult reste sous-traitant pour cette conservation.

11.2 Le Cabinet choisit lui-même quand ses données sont effacées. Sur demande écrite d'un administrateur, Nena Consult efface les données du Cabinet de la base de données active dans les 30 jours. Elles disparaissent des sauvegardes selon la politique de conservation, donc au plus tard 12 mois après. Nena Consult confirme l'effacement par écrit. Ce qu'elle doit conserver légalement, comme les factures au Cabinet, reste conservé.

11.3 Le Cabinet réalise lui-même un export complet avant cette demande, et règle la suite de la conservation, du transfert ou de la destruction de ses dossiers selon les règles de sa profession. Le délai légal de conservation du dossier patient incombe au prestataire de soins, pas à Nena Consult.

11.4 Si Nena Consult arrête Horalena, l'article 10.3 des conditions d'utilisation s'applique : un avis au moins 12 mois à l'avance, afin que le Cabinet puisse emporter ses données. Ensuite, Nena Consult efface les données.

11.5 Si Nena Consult met fin au contrat avec un Cabinet (article 10.1 ou 10.2 des conditions d'utilisation), le Cabinet peut encore se connecter, consulter et exporter pendant au moins 90 jours après la fin. Nena Consult n'efface les données qu'ensuite, et seulement après avoir prévenu les administrateurs au moins deux fois par e-mail, la dernière fois au moins 30 jours à l'avance.

Article 12. Responsabilité

12.1 Chaque partie est responsable comme le prévoit l'article 82 du RGPD. Les limitations des conditions d'utilisation s'appliquent aussi à ce contrat, sauf envers les personnes concernées et pour autant que la loi ne le permette pas.

Article 13. Modifications

13.1 Nena Consult peut, pour un motif valable, modifier ce contrat au moyen d'une nouvelle version. Elle annonce une nouvelle version au moins 30 jours à l'avance aux administrateurs, sauf si la loi ou une raison de sécurité urgente impose un délai plus court. Une nouvelle version ne réduit pas le niveau de protection. L'administrateur l'accepte dans Horalena. Chaque acceptation est conservée avec la version, la date et l'utilisateur. Si le Cabinet n'est pas d'accord, l'article 18.2 des conditions d'utilisation s'applique.

Article 14. Droit applicable

14.1 Le droit belge s'applique à ce contrat. Les litiges relèvent de la compétence du tribunal de l'entreprise de Gand, division Gand.

Annexe A. Description du traitement

Finalité. Fournir un logiciel de cabinet aux prestataires de soins : agenda, prise de rendez-vous en ligne, liste d'attente, rappels, fichier patients, dossier, administration INAMI, notes d'honoraires et paiements, site du cabinet, portail patient, invitations et rôle de garde, pour autant que ce soit compris dans la formule du Cabinet.

Nature. Conserver, organiser, consulter, afficher, modifier, envoyer des messages sur instruction, exporter.

Durée. Aussi longtemps que le contrat court, et ensuite selon l'article 11 et l'annexe D.

Personnes concernées. Patients, leurs parents, représentants et personnes de contact ; payeurs d'une note d'honoraires ; visiteurs qui envoient un message ou prennent rendez-vous via le site du Cabinet ; utilisateurs du Cabinet (prestataires de soins, accueil, administrateurs) ; membres d'un rôle de garde, y compris en dehors du Cabinet ; prescripteurs et autres prestataires de soins mentionnés dans un dossier ; stagiaires. Le Cabinet peut donner à son comptable un lien vers un dossier de recettes.

Type de données	Exemples	Catégorie particulière ?
Identification et contact	nom, date de naissance, sexe, adresse, adresse e-mail, téléphone, langue, personne de contact	non, mais souvent révélateur dans ce contexte
Numéro de registre national	NISS, et champs de l'eID (numéro de carte, validité, nationalité), jamais la photo	cadre légal distinct
Rendez-vous	moment, prestataire de soins, type, motif de la visite si le Cabinet le demande, présence, liste d'attente	santé (déductible)
Dossier	notes, rapports, bilans, pièces jointes, questionnaires, consentements, programmes d'exercices, schéma dentaire, évaluations de Katz, plaies, grossesse, médication, laboratoire, vaccinations, déclarations de volonté	santé
Administration	prescriptions, diagnostic sur une prescription, prestations INAMI, attestations de soins donnés, accords, mutualité, statut	santé
Financier	notes d'honoraires, paiements, demandes de paiement, mouvements bancaires (nom, numéro de compte, communication)	partiellement déductible
Messages	messages du portail, formulaire de contact, contenu des e-mails et SMS	peut contenir des données de santé
Utilisateurs	nom, e-mail, rôle, numéro INAMI, données de double authentification, certificat eHealth et le NISS qu'il contient	non
Rôle de garde	nom, contact, tours de garde, indisponibilités, heures prestées	non
Technique	adresse IP sous forme de code avec clé dans le journal d'audit, code visiteur temporaire pour les statistiques, journaux du serveur web (adresse IP, heure, page, navigateur)	non

Annexe B. Mesures techniques et organisationnelles

Séparation entre cabinets

Tous les cabinets se trouvent dans une seule base de données, séparés logiquement : les données liées à un cabinet reçoivent automatiquement un filtre sur le cabinet, et sans contexte de cabinet, une requête ne renvoie rien.

Accès

- La double authentification est obligatoire pour chaque utilisateur du Cabinet.
- Mots de passe d'au moins 12 caractères avec majuscules, minuscules et chiffres, conservés sous forme de hachage bcrypt, avec un contrôle des mots de passe divulgués.
- Au maximum 5 tentatives de connexion par minute par adresse et IP, et 30 par IP. Sessions chiffrées, cookie uniquement via https, fin après 240 minutes. Il n'y a pas de fonction pour rester connecté.
- Rôles : seul un prestataire de soins ouvre le dossier, jamais l'accueil. Les paramètres uniquement l'administrateur.
- Les patients n'ont pas de mot de passe : ils reçoivent par e-mail un lien dont seul le hachage est conservé, valable 30 minutes, ou 7 jours dans un e-mail signalant que quelque chose est disponible. La session s'arrête après 30 minutes d'inactivité et dure au maximum 12 heures. Les personnes ayant la même adresse e-mail dans un cabinet relèvent de la même connexion (prévu pour une famille).
- Les membres d'un rôle de garde n'ont pas de compte mais un lien personnel.
- L'écran de gestion de Nena Consult exige la double authentification et affiche des comptages et aucune donnée de patient. Ce que Nena Consult y modifie figure dans le journal d'audit. L'accès au serveur n'est possible qu'avec une clé SSH, et ne figure pas dans le journal d'audit de l'application.

Chiffrement

- Pendant le transport : https avec HSTS.
- Dans la base de données, champ par champ, avec AES-256 : notamment le titre et le contenu du dossier, le numéro de registre national, le contenu des messages, le formulaire de contact, les tâches, les notes du jour, le contenu des notes d'honoraires, le nom et le compte des extraits bancaires.
- Pas chiffrés champ par champ, mais protégés par l'accès à la base de données : le nom, la date de naissance, le sexe, l'e-mail, le téléphone et l'adresse du patient, le motif de la visite, le destinataire et l'objet d'un message, le moment et le prestataire de soins d'un rendez-vous.
- Les pièces jointes du dossier sont chiffrées sur disque, en dehors de la racine web. Le certificat eHealth est chiffré avec une clé propre à chaque cabinet.
- La clé de l'application se trouve sur le même serveur que la base de données. Le chiffrement par champ protège donc contre celui qui n'a que la base de données ou une copie de celle-ci, pas contre celui qui a tout le serveur ou l'administrateur.

Journal d'audit

Via l'application, une ligne ne peut être ni modifiée ni effacée. L'ouverture d'une fiche, d'un dossier ou d'une pièce jointe est enregistrée, l'adresse IP uniquement sous forme de code avec clé. Le patient voit dans le portail qui a ouvert son dossier, avec le nom et la fonction : les 200 dernières lignes, sans les lignes sur les rendez-vous, les séries, la liste d'attente et les rappels. L'ouverture d'un agenda ou d'une liste de patients n'est pas enregistrée par patient.

Sauvegarde et restauration

- Chaque nuit, une sauvegarde chiffrée de la base de données et des fichiers privés (AES-256-GCM, une clé propre à chaque archive). Chaque dimanche, la plus récente est entièrement déchiffrée et recalculée.
- Politique de conservation : la plus récente de chacun des 14 derniers jours, 8 dernières semaines et 12 derniers mois.
- Les archives se trouvent sur le même serveur. Nena Consult en récupère régulièrement une copie chiffrée sur son propre appareil. La restauration sur une installation vierge a été exercée. La restauration sur un vrai nouveau serveur n'a pas encore été exercée, donc la durée d'une véritable panne n'est pas mesurée.

Surveillance et sécurité web

Chaque heure, un contrôle du planificateur, de la sauvegarde, de l'espace disque, de la file d'attente et de la base de données, avec un e-mail à Nena Consult en cas de problème. Une Content-Security-Policy limitée à nos propres sources, et les pages connectées ne vont pas dans le cache du navigateur. Une photo eID n'est jamais conservée.

Messages

Les e-mails et SMS passent par une file d'attente propre ; le contenu est chiffré et effacé après 30 jours. Un SMS contient le cabinet, le moment et un lien court, jamais le motif ni la profession. Un e-mail de rendez-vous contient le cabinet, le moment, le prestataire de soins, le lieu et les informations ajoutées par le Cabinet, ni diagnostic ni rapport. Une invitation contient le texte écrit par le Cabinet.

Ce qui n'existe pas (encore)

Ceci figure ici pour que personne ne le lise comme une promesse.

- Un test de sécurité indépendant. Il y a bien eu un exercice interne les 2 et 3 novembre 2026, dont les erreurs graves ont été corrigées. Ce n'est pas un test indépendant.
- Une certification, comme ISO 27001.
- Un coffre-fort de clés (KMS).
- Un deuxième centre de données pour les sauvegardes.
- Un journal des accès au serveur par l'administrateur que le Cabinet peut consulter. Pour cela, l'article 3.3 s'applique.
- Un délégué à la protection des données : aucun n'a été désigné. Les questions vont à team@horalena.be.

Annexe C. Sous-traitants ultérieurs

Partie	Ce qu'elle fait	Quelles données	Où
Combell SA, Skaldenstraat 121, 9042 Gand (Managed VPS)	hébergement du serveur, de la base de données, des fichiers et des sauvegardes	tout ce qui se trouve dans Horalena, chiffré ou non	Union européenne. Les adresses IP sont au nom de TransIP B.V. (Leyde, Pays-Bas). Nena Consult complète ici le centre de données exact dès que l'hébergeur le confirme.
Google Workspace	envoie les e-mails de l'application	destinataire, objet avec le nom du cabinet, contenu de l'e-mail (moment, prestataire de soins, lieu, liens, le texte d'une invitation)	Google est une entreprise américaine ; voir l'article 6.2

Partie	Ce qu'elle fait	Quelles données	Où
Brevo (Sendinblue SAS, Paris)	envoie les SMS, uniquement pour ceux qui utilisent le service SMS d'Horalena	numéro de téléphone et contenu du SMS	France

Si un Cabinet utilise son propre compte Brevo, Brevo est son propre sous-traitant et Horalena ne fait que transmettre l'instruction. Cloudflare gère uniquement le DNS de horalena.be, sans proxy : le trafic n'y passe pas, ce n'est donc pas un sous-traitant ultérieur. eHealth, MyCareNet et Recip-e ne reçoivent rien aujourd'hui (simulateur) ; plus tard, ce seront des destinataires sur instruction du prestataire de soins, pas des sous-traitants ultérieurs.

Annexe D. Délais de conservation

Donnée	Délai	Ce qui se passe
Dossier patient, y compris les versions et les éléments barrés	pas de délai automatique ; l'obligation de conservation de 30 à 50 ans incombe au prestataire de soins	jamais effacé de lui-même ; voir l'article 11
Fiche patient, rendez-vous, prestations, attestations de soins donnés, notes d'honoraires et paiements, journal d'audit	pas de délai automatique	restent jusqu'à ce que le Cabinet les fasse effacer (article 11)
Contenu des e-mails et SMS	30 jours	contenu effacé ; le destinataire, l'objet, le type et l'heure restent
Message via le formulaire de contact du site	12 mois	effacé
Fichier d'importation téléversé, extrait bancaire	24 heures	fichier effacé ; ce qui a été importé reste
Export d'un cabinet entier	72 heures, ou plus tôt avec « Supprimer maintenant »	fichier et clé effacés
Lien de connexion au portail	30 jours après l'expiration	effacé
MyCareNet et Recip-e : demande et réponse	90 jours	contenu effacé ; le résumé et la référence restent
Patient en ligne qui n'a jamais confirmé	30 jours	identité anonymisée
Liste d'attente	2 jours sans confirmation, sinon 90 jours	expire ; la ligne reste jusqu'à ce que le Cabinet la fasse effacer
Statistiques de visite du site	mesures brutes 3 jours au maximum, compteurs journaliers 24 mois	effacées
Journaux du serveur web	90 jours au maximum	effacés
Journal de l'application	14 jours	effacé
Sauvegardes	14 jours, 8 semaines, 12 mois	ce qui est effacé dans la base de données n'y figure plus non plus au plus tard 12 mois après