

Politique de confidentialité des services Nicolab

Dernière modification le 13 septembre 2023

1. Introduction

Chez Nicolab, nous respectons la confidentialité de vos informations que nous sommes susceptibles de collecter dans le cadre de nos services. Les données à caractère personnel désignent les informations qui peuvent vous identifier directement ou indirectement, vous ou d'autres personnes (« données à caractère personnel »), par exemple votre prénom, votre nom ou votre adresse électronique.

Nous ne divulguons pas vos données à caractère personnel à des tiers, sauf à nos filiales et aux sous-traitants qui nous assistent dans la prestation de nos services ou aux autorités si nous sommes tenus d'obéir à des lois ou à des ordonnances judiciaires. Avec votre consentement, nous utilisons des cookies à des fins de marketing, de performance et de statistiques.

Vous avez toujours le droit de demander gratuitement des informations sur vos données à caractère personnel stockées, leur origine, leurs destinataires et le but de leur collecte. Vous avez également le droit de demander qu'elles soient corrigées, bloquées ou supprimées. Vous pouvez nous contacter à tout moment à l'adresse de notre délégué à la protection des données indiquée ci-dessous si vous avez d'autres questions sur le sujet de la confidentialité et de la protection des données. Vous pouvez bien entendu également déposer une plainte auprès des autorités de réglementation compétentes.

2. Dispositions générales

La présente politique de confidentialité des services Nicolab s'applique aux données à caractère personnel traitées par Nicolab (ci-après, « nous », « nos ») dans le cadre du fonctionnement et des services que nous vous proposons via nos services d'abonnement, l'application StrokeViewer et le site Internet (nicolab.com) (collectivement appelés « Services »). La présente politique de confidentialité des services Nicolab explique quelles données à caractère personnel peuvent être collectées, comment nous les utilisons, comment vous pouvez exercer vos droits et dans quelles circonstances nous pouvons divulguer ces données à caractère personnel à des tiers. Nous traitons également les données des patients pour le compte de votre organisation, avec laquelle nous avons conclu un contrat de sous-traitance des données distinct.

Les données à caractère personnel sont gérées par NICO-Lab B.V., inscrite au registre du commerce de la Chambre de commerce d'Amsterdam sous le numéro d'enregistrement (KvK) : 64531775, dont le siège social et l'adresse de signification sont situés Paasheuvelweg 25, 1105 BP, Amsterdam, Pays-Bas.

Nicolab a désigné un délégué à la protection des données qui peut être contacté à l'adresse suivante : infosec@nicolab.com.

Nous traitons vos données à caractère personnel pour pouvoir vous fournir les services¹, y compris, mais sans s'y limiter :

- Analyse automatique d'images DICOM à l'aide des algorithmes de StrokeViewer
- Visionneuse DICOM Web
- Visionneuse DICOM mobile

¹ La liste complète des services est fournie dans le Contrat principal et peut être différente pour chaque partie.

- Partage d'images à l'échelle du réseau
- Messagerie instantanée
- Assistance technique en cas de dysfonctionnements ou dans d'autres cas lorsque cela est jugé nécessaire
- Prestations de formation

Les données à caractère personnel fournies via les services seront traitées conformément aux lois applicables en matière de protection des données.

En utilisant nos services, vous acceptez que nous traitions vos données à caractère personnel conformément aux conditions énoncées dans la présente politique de confidentialité des services Nicolab.

De plus, un contrat distinct entre nous et notre client régit la livraison, l'accès à et l'utilisation des services (le « Contrat principal »), y compris le traitement de toutes les données à caractère personnel, tous les fichiers ou autres contenus fournis via l'utilisation des services (collectivement, « Données client »). L'organisation (par ex. votre employeur ou une autre entité ou personne) qui a conclu le Contrat principal (« Client ») contrôle certains aspects de son utilisation des Services (leur « Déploiement ») et des Données client associées, par exemple, combien de temps Nicolab conservera les Données client.

Dans la mesure où le traitement de vos données à caractère personnel est fondé sur votre consentement, nous ne modifierons pas la portée de ce traitement, à moins que vous n'ayez donné un consentement supplémentaire à la modification de la portée de ce traitement.

Si vous êtes employé par un client, la présente politique de confidentialité des services Nicolab ainsi que le Contrat principal définissent les dispositions et les politiques régissant votre utilisation de nos services.

3. Portée des données à caractère personnel collectées et traitées

Nous pouvons traiter les données à caractère personnel suivantes en conséquence de notre Contrat principal ou si Nicolab accorde l'accès à des personnes pour un déploiement (« Utilisateurs autorisés »). De plus, nous pouvons collecter des données sur les paramètres de l'application tels que les préférences de notification et la méthode de connexion préférée.

Données à caractère personnel des utilisateurs autorisés collectées pour permettre aux utilisateurs autorisés d'utiliser les services :

1. Données collectées dans le cadre de la prestation de services :
 - Nom et prénom
 - Titre du poste
 - Employeur
 - Adresse électronique
 - Numéro de téléphone portable (optionnel)
 - Adresse IP
 - Cookies de session
2. Données collectées en cas d'accès mobile aux services :
 - Profil de l'appareil mobile²
 - Préférences dans l'application³
 - Code PIN de l'application (optionnel)
3. Données collectées via le service de messagerie instantanée :
 - Textes et médias transmis

StrokeViewer est accessible via un navigateur ou une application mobile avec le domaine national spécifique de Strokeviewer.com (par ex. aux Pays-Bas nl.Strokeviewer.com).

Les utilisateurs autorisés doivent d'abord suivre une formation avant d'utiliser les services. Le contenu de la formation peut différer en fonction de la description de poste de l'utilisateur autorisé et les informations sur la formation seront communiquées par courrier électronique.

Nicolab propose une assistance pour les problèmes techniques liés à l'utilisation des services. Lorsque le service d'assistance est contacté, les informations suivantes peuvent être collectées pour mieux vous aider à résoudre le problème.

Donnée supplémentaire :

- Données de journal : comme pour la plupart des services technologiques fournis via Internet, nos serveurs collectent automatiquement des informations lorsque vous accédez à ou utilisez nos services et les enregistrent dans des fichiers journaux.
- Données client : les déploiements sont configurés pour envoyer des données client à Nicolab pour l'utilisation des services, par exemple des études par tomodensitométrie numérique (TDM) peuvent être envoyées à Nicolab via les services afin que l'algorithme d'une intelligence artificielle détecte des affections suspectées telles qu'une occlusion des gros vaisseaux. Les données client peuvent inclure des données concernant la santé. Ces données sensibles nécessitent des niveaux de protection plus élevés. Nous devons disposer de justifications supplémentaires pour la collecte, le stockage et l'utilisation de ce type d'informations personnelles. Ces données sensibles sont régies par le Contrat principal et le contrat de sous-traitance des données entre le client et Nicolab et non par la présente politique de confidentialité des services Nicolab.

Nous pouvons également utiliser votre adresse électronique pour vous envoyer des études post-mise sur le marché sur la base de notre intérêt légitime. Si vous ne souhaitez pas que votre adresse électronique soit utilisée à cette fin, vous pouvez toujours vous opposer à ce traitement.

2 Le profil de l'appareil mobile désigne la collecte de diverses données sur l'appareil d'un utilisateur autorisé et la façon dont cet appareil est utilisé, y compris, mais sans s'y limiter : l'adresse IP, le pays et l'opérateur, la marque et le modèle de l'appareil, la version du système d'exploitation de l'appareil, les préférences linguistiques.

3 Les préférences dans l'application désignent les paramètres de l'application mobile configurés individuellement par un utilisateur autorisé, y compris, mais sans s'y limiter : préférences pour le code PIN ou la connexion rapide biométrique, les notifications push (on/off), jetons push (un jeton par lequel le téléphone mobile de l'utilisateur autorisé peut être ciblé pour les notifications push).

4. Finalité et base légale de la collecte des données à caractère personnel

La législation applicable en matière de protection des données permet à Nicolab de traiter vos données à caractère personnel aux fins de prestation des services, telles que définies dans le Contrat principal concerné (votre employeur) ou sur la base de votre consentement.

5. Durée de conservation des données à caractère personnel

Les données à caractère personnel sont conservées pendant le temps nécessaire à l'exécution, à la résiliation ou à l'expiration d'un Contrat principal et jusqu'à ce que nos obligations légales de conservation des enregistrements aient expiré. Des dispositions supplémentaires sur la durée de stockage des données sont prises dans le cadre du Contrat principal.

6. Sous-traitance

6.1. Prestataires de services (sous-traitants)

Afin d'assurer le bon fonctionnement des services, y compris l'exécution du Contrat principal, Nicolab utilise des services externes (tels que des logiciels tiers). Nous n'utilisons que des services fournis par des sous-traitants susceptibles de garantir que des mesures techniques et organisationnelles appropriées sont mises en œuvre pour assurer la conformité du traitement des données à caractère personnel aux exigences de la législation applicable en matière de protection des données et pour protéger les droits des personnes auxquelles les données se rapportent. Avant de divulguer des données à caractère personnel à des tiers, nous concluons un contrat de (sous-)traitance leur imposant des normes de sécurité appropriées.

Nicolab ne divulgue les données à caractère personnel que si cela s'avère nécessaire pour une finalité spécifique du traitement des données et uniquement dans la mesure où cela s'avère nécessaire pour atteindre cette finalité. Les données à caractère personnel de l'utilisateur autorisé de nos services pourront être divulguées aux prestataires de services afin de nous fournir les solutions techniques, informatiques et organisationnelles nécessaires pour que Nicolab puisse exercer son activité commerciale. Nous divulguons les données à caractère personnel de l'utilisateur autorisé à un prestataire engagé uniquement si et dans la mesure où cela s'avère nécessaire pour atteindre une finalité spécifique du traitement des données dans le cadre de la présente.

6.2. Autres destinataires (responsables du traitement)

Nous pouvons partager vos données à caractère personnel avec les responsables de traitement suivants (c'est-à-dire des tiers qui traitent vos données à caractère personnel à leurs propres fins) :

- les forces de l'ordre ou d'autres organismes si nous y sommes tenus par la loi, ou par un mandat, une assignation à comparaître ou une ordonnance judiciaire de divulgation de vos données à caractère personnel.

7. Transfert transfrontalier de données

Le transfert des données à caractère personnel fournies dans le cadre des services est conforme à la législation nationale et internationale.

8. Droits de la personne à laquelle les données à caractère personnel se rapportent

Vous disposez des droits décrits ci-dessous sur vos données à caractère personnel.

- Droit d'accès, de rectification, de limitation, de suppression ou de déplacement des données à caractère personnel : la personne à laquelle les données à caractère personnel se rapportent a le droit de nous demander de lui fournir l'accès à ses données à caractère personnel, de faire rectifier ou de supprimer ces données à caractère personnel (« le droit à l'oubli »), de limiter ou de s'opposer au traitement de celles-ci, ainsi que de faire déplacer ses données à caractère personnel.
- Droit de retirer le consentement à tout moment : la personne dont les données à caractère personnel sont traitées par Nicolab sur la base de son consentement a le droit de retirer son consentement à tout moment, et cela n'affectera pas le droit de traiter ces données à caractère personnel sur la base du consentement avant le retrait de celui-ci.

- Droit de déposer une plainte : la personne dont les données à caractère personnel sont traitées par Nicolab a le droit de déposer une plainte auprès de l'Autoriteit Persoonsgegevens, l'autorité de contrôle néerlandaise.
- Droit d'opposition : la personne dont les données à caractère personnel sont traitées a le droit de s'opposer à tout moment au traitement de ses données à caractère personnel.

Vous pouvez exercer vos droits en nous contactant à l'adresse infosec@nicolab.com afin que nous puissions examiner votre demande conformément à la loi applicable. Lorsque nous recevons votre demande relative à vos droits par courrier électronique, vous acceptez que nous puissions prendre des mesures pour vérifier votre identité avant de répondre à la demande afin de protéger votre confidentialité et votre sécurité, par exemple en vous contactant ou en contactant votre employeur afin d'établir votre identité et votre qualification en tant qu'utilisateur autorisé.

9. Sécurité

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement des données et du risque, quel que soit son caractère probable et imminent, de violer les droits ou libertés des personnes physiques, Nicolab met en œuvre des mesures techniques et organisationnelles appropriées pour conformer le traitement des données aux lois applicables en matière de protection des données et pouvoir le démontrer. Nos mesures de sécurité sont continuellement améliorées à mesure que la technologie évolue.

9.1. Mesures techniques

Nicolab prend des mesures techniques pour empêcher des personnes non autorisées d'intercepter ou de modifier les données à caractère personnel transmises par voie électronique. Nicolab est certifié ISO 27001 et ISO 13485.

9.2. Liens vers des sites externes

Nos services peuvent comporter des hyperliens vers des sites Internet externes ne nous appartenant pas. Si vous cliquez sur un lien tiers, vous serez redirigé vers le site de ce tiers. Une fois que vous avez quitté nos services, nous ne pouvons plus être tenus responsables de la protection et de la confidentialité des informations que vous fournissez. Nous vous conseillons fortement de consulter la politique de confidentialité des services Nicolab et les conditions générales de tout site Internet que vous visitez. Nous n'avons aucun contrôle sur et n'assumons aucune responsabilité quant au contenu, aux politiques ou pratiques en matière de confidentialité de tout site, produit ou service tiers.

9.3. Authentification et autorisation des utilisateurs autorisés

L'authentification des utilisateurs autorisés est entièrement gérée par le système fournisseur d'identité de l'hôpital, tel qu'un serveur de fichiers Active Directory (ADFS). Ainsi, l'hôpital exerce un contrôle total sur la détermination des politiques de mot de passe, l'accès d'utilisateurs autorisés à StrokeViewer, l'application de l'authentification multifacteur, etc. Ainsi, lorsqu'un utilisateur autorisé tente d'accéder à StrokeViewer, cet utilisateur autorisé est redirigé vers le système fournisseur d'identité de l'hôpital. Si le système fournisseur d'identité utilisé par l'hôpital ne prend pas en charge l'authentification à deux facteurs, l'hôpital peut utiliser l'application StrokeViewer pour fournir une authentification à deux facteurs.

Une fois authentifié, un utilisateur autorisé dispose des autorisations suivantes :

- 1 heure d'accès en ligne au produit ;
- 336 heures (14 jours) d'accès mobile au produit.

Passé ce délai, l'utilisateur autorisé est invité à s'authentifier à nouveau. Des mesures de sécurité supplémentaires sont également appliquées :

- si le compte de l'utilisateur autorisé est suspendu ou révoqué par le fournisseur d'identité du client, son accès au produit est automatiquement résilié au plus tard 1 heure après ;
- l'application mobile nécessite que l'utilisateur autorisé fournisse un code PIN ou des données biométriques supplémentaires pour l'authentification ;
- l'accès à Internet est automatiquement verrouillé après 20 minutes d'inactivité pour empêcher tout accès non autorisé aux sessions sans surveillance ; pour le déverrouiller, l'utilisateur autorisé doit s'authentifier à nouveau ;

- si l'utilisateur autorisé passe à un autre onglet du navigateur ou à une autre fenêtre et ne revient pas à la page Internet du produit dans les 10 minutes, son accès en ligne est verrouillé même si l'utilisateur autorisé continue de travailler avec les autres applications et/ou onglets du navigateur ; pour le déverrouiller, l'utilisateur autorisé doit s'authentifier à nouveau ;
- l'accès mobile est automatiquement verrouillé après 1 minute d'inactivité pour empêcher tout accès non autorisé aux sessions sans surveillance ; pour le déverrouiller, l'utilisateur autorisé doit fournir un code PIN ou des données biométriques supplémentaires.

10. Violation des données à caractère personnel et obligation de notification

En cas de violation des données à caractère personnel dans le cadre des services fournis par Nicolab, Nicolab informera rapidement les utilisateurs autorisés concernés et, le cas échéant, les autorités de contrôle compétentes, si la violation des données à caractère personnel présente un risque pour les droits et libertés des utilisateurs autorisés affectés. La notification sera effectuée sans retard injustifié dès la prise de connaissance de la violation, mais au plus tard dans un délai de 72 heures. En cas de violation de données à caractère personnel, Nicolab prendra toutes les mesures raisonnables pour limiter les conséquences de la violation des données à caractère personnel et/ou empêcher qu'une telle violation survienne à nouveau, contre paiement des frais raisonnables par vous.

11. Modifications de la politique de confidentialité des services Nicolab

Nicolab se réserve le droit de modifier, amender ou changer la présente politique de confidentialité des services Nicolab à tout moment et à sa seule discrétion. De tels changements peuvent être mis en œuvre par Nicolab sans préavis. Nicolab encourage les visiteurs à consulter fréquemment cette page pour obtenir les dernières informations sur nos pratiques en matière de confidentialité et pour toute mise à jour ou révision. La poursuite de votre utilisation de ce site après tout changement apporté à la présente politique de confidentialité des services Nicolab constituera votre acceptation de cette modification.

Détails des données à caractère personnel

Description des prestations	<p>StrokeViewer est une application de traitement d'images de type logiciel en tant que service (Software as a Service, SaaS). StrokeViewer analyse automatiquement les imageries reçues des patients présentant des symptômes d'accident vasculaire cérébral. Après l'analyse, un rapport est généré qui inclut les caractéristiques des images concernant l'AVC. Ces fonctionnalités peuvent être utilisées par le médecin en tant qu'outil d'assistance pour des diagnostics plus approfondis.</p> <ol style="list-style-type: none"> 1. Analyse automatique d'images DICOM à l'aide des algorithmes de StrokeViewer 2. Visionneuse Web DICOM, 3. Visionneuse DICOM mobile 4. Partage d'images à l'échelle du réseau 5. Messagerie instantanée 6. Assistance technique en cas de dysfonctionnements ou dans d'autres cas lorsque cela est jugé nécessaire 7. Prestations de formation
Type de données à caractère personnel	<ol style="list-style-type: none"> 1. Données à caractère personnel des utilisateurs autorisés, à l'exclusion de catégories particulières de données à caractère personnel (RGPD Art.4,9)
Catégories de personnes impliquées	<ol style="list-style-type: none"> 1. Utilisateurs autorisés
Finalités du traitement	<p>Le traitement n'aura lieu que dans le cadre et pendant la durée du Contrat Principal aux fins de :</p> <ul style="list-style-type: none"> - Prestation de services - Communication - Diagnostic et résolution des problèmes - Personnalisation et individualisation - Analyse et recherche - Observance de la législation
Responsables du traitement approuvés	<p>Google Cloud, Stream.io</p>
Période de conservation	<ol style="list-style-type: none"> 1. L'enregistrement du journal sera conservé aussi longtemps que le contrat avec le client sera en vigueur, mais pour une durée maximale de 5 ans.