

Privacybeleid van Nicolab Services

Laatst gewijzigd 13-Sep-2023

1. Inleiding

Bij Nicolab respecteren we uw privacy met betrekking tot alle informatie die we verzamelen tijdens het uitvoeren van onze diensten. Persoonsgegevens betekenen informatie waarmee u of andere personen direct of indirect kunnen worden geïdentificeerd ('Persoonsgegevens'), bijvoorbeeld voornaam, achternaam of e-mailadres.

Wij maken uw persoonsgegevens niet bekend aan derden, behalve aan onze dochterondernemingen en aan gegevensverwerkers die ons helpen bij het leveren van onze diensten of aan autoriteiten als we ons moeten houden aan wetten of gerechtelijk bevel(en). Met uw toestemming gebruiken wij cookies voor marketing-, prestatie- en statistische doeleinden.

U heeft altijd het recht om kosteloos informatie op te vragen over uw opgeslagen persoonsgegevens, de herkomst ervan, de ontvangers ervan en het doel van de verzameling ervan. U heeft ook het recht om te verzoeken dat deze worden gecorrigeerd, geblokkeerd of verwijderd. Als u nog vragen heeft over de kwestie van privacy en gegevensbescherming, kunt u op elk gewenst moment contact met ons opnemen via het onderstaande adres van onze functionaris voor gegevensbescherming. Uiteraard kunt u ook een klacht indienen bij de bevoegde regelgevende autoriteiten.

2. Algemene bepalingen

Dit privacybeleid van Nicolab Services is van toepassing op persoonsgegevens die worden verwerkt door Nicolab (hierna "ons", "wij") in verband met de werking en diensten die wij u aanbieden via onze abonnementsdiensten, de StrokeViewer-app en de website (nicolab.com). (gezamenlijk "Diensten" genoemd). In dit privacybeleid van Nicolab Services wordt uitgelegd welke persoonsgegevens kunnen worden verzameld, hoe we deze gebruiken, hoe u uw rechten kunt uitoefenen en onder welke omstandigheden we deze persoonsgegevens aan derden kunnen bekendmaken. Ook namens uw organisatie verwerken wij patiëntgegevens. Hiervoor hebben wij met uw organisatie een aparte verwerkersovereenkomst afgesloten.

Persoonsgegevens worden beheerd door NiCo-Lab B.V., ingeschreven in het handelsregister van de Kamer van Koophandel te Amsterdam onder registratienummer (KvK): 64531775, met vestigingsplaats en domicilie aan de Paasheuvelweg 25, 1105 BP, Amsterdam, Nederland.

Nicolab heeft een functionaris voor gegevensbescherming aangesteld die gecontacteerd kan worden op het volgende adres: infosec@nicolab.com.

Wij verwerken uw persoonsgegevens om u de Diensten¹ te kunnen leveren, inclusief maar niet beperkt tot:

- Automatische analyse van DICOM-afbeeldingen met behulp van StrokeViewer-algoritmen
- Web DICOM-viewer
- Mobiele DICOM-viewer
- Netwerkbreed delen van afbeeldingen

¹ De volledige lijst met diensten is opgenomen in de hoofdovereenkomst en kan voor iedere partij verschillend zijn.

- Instant messaging
- Technische ondersteuning bij storingen of in andere gevallen wanneer dit noodzakelijk wordt geacht
- Opleidingsdiensten

Persoonsgegevens die via de diensten worden ingediend, worden verwerkt in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming.

Door onze diensten te gebruiken, gaat u ermee akkoord dat wij uw persoonsgegevens verwerken in overeenstemming met de voorwaarden uiteengezet in dit privacybeleid van Nicolab Services.

Bovendien regelt een afzonderlijke overeenkomst tussen ons en onze klant de levering, de toegang en het gebruik van de diensten (de "Hoofdovereenkomst"), inclusief de verwerking van persoonsgegevens, bestanden of andere inhoud die wordt ingediend via het gebruik van de diensten (gezamenlijk: "Klantgegevens"). De organisatie (bijv. uw werkgever of een andere entiteit of persoon) die de hoofdovereenkomst is aangegaan ("Klant") controleert bepaalde aspecten van hun gebruik van de diensten (hun "Inzet") en bijbehorende klantgegevens, bijvoorbeeld hoelang Nicolab klantgegevens zal bewaren.

Voor zover de verwerking van uw persoonsgegevens gebaseerd is op uw toestemming, zullen wij de reikwijdte van een dergelijke verwerking niet wijzigen, tenzij u aanvullende toestemming heeft gegeven voor de gewijzigde reikwijdte van een dergelijke verwerking.

Als u bij een klant in dienst bent, worden in dit privacybeleid van Nicolab Services samen met de hoofdovereenkomst de bepalingen en het beleid uiteengezet die van toepassing zijn op uw gebruik van onze diensten.

3. Reikwijdte van de verzamelde en verwerkte persoonsgegevens

We kunnen de volgende persoonsgegevens verwerken als gevolg van onze hoofdovereenkomst of het verlenen van toegang door Nicolab aan individuen tot een implementatie ("Geautoriseerde gebruikers"). Daarnaast kunnen we gegevens verzamelen over instellingen in de app, zoals meldingsvoorkeuren en voorkeursmethode voor inloggen.

Persoonsgegevens van geautoriseerde gebruikers verzameld om geautoriseerde gebruikers in staat te stellen de diensten te gebruiken:

1. Gegevens verzameld binnen de dienstverlening:
 - Voor- en achternaam
 - Functietitel
 - Werkgever
 - E-mailadres
 - Mobiel telefoonnummer (optioneel)
 - IP-adres
 - Sessiecookies

2. Gegevens verzameld bij mobiele toegang tot de diensten:
 - Profiel van mobiel apparaat²
 - Applicatievoorkeuren³
 - Pincode applicatie (optioneel)

3. Gegevens verzameld binnen de instant messaging-service:
 - Tekst en media doorgestuurd

StrokeViewer is toegankelijk via een browser of mobiele applicatie met het landspecifieke domein van strokeviewer.com (bijv. in Nederland nl.strokeviewer.com).

Geautoriseerde gebruikers moeten eerst een opleiding volgen voordat zij gebruik kunnen maken van de diensten. De inhoud van de opleiding kan verschillen, afhankelijk van de functiebeschrijving van de geautoriseerde gebruiker. Informatie over de opleiding wordt via e-mail gecommuniceerd.

Nicolab biedt ondersteuning bij technische problemen met betrekking tot het gebruik van de diensten. Wanneer contact wordt opgenomen met de supportdesk, kunnen de volgende gegevens worden verzameld om het probleem beter te kunnen oplossen.

Aanvullende gegevens:

- Loggegevens: zoals bij de meeste technologische diensten die via internet worden geleverd, verzamelen onze servers automatisch informatie wanneer u onze diensten bezoekt of gebruikt en leggen deze vast in logbestanden.
- Klantgegevens: implementaties zijn geconfigureerd om klantgegevens naar Nicolab te sturen voor het gebruik van de diensten. Zo kunnen digitale computertomografie (CT)-onderzoeken via de diensten naar Nicolab worden verzonden, zodat een algoritme voor kunstmatige intelligentie vermoedelijke aandoeningen zoals occlusie van een groot vat kunnen detecteren. Klantgegevens kunnen gegevens over de gezondheid omvatten. Dergelijke gevoelige gegevens vereisen een hoger beschermingsniveau. We moeten een verdere rechtvaardiging hebben voor het verzamelen, opslaan en gebruiken van dit soort persoonlijke informatie. Dergelijke gevoelige gegevens vallen onder de hoofdovereenkomst en de gegevensverwerkingsovereenkomst tussen de klant en Nicolab, en niet onder dit privacybeleid van Nicolab Services.

We kunnen uw e-mailadres ook gebruiken om u marktonderzoeken te sturen op basis van ons legitieme belang. Als u niet wilt dat uw e-mailadres voor dit doel wordt gebruikt, kunt u altijd bezwaar maken tegen deze verwerking.

² Het profiel van een mobiel apparaat is de verzameling van een verscheidenheid aan gegevens over het apparaat van een geautoriseerde gebruiker en de manier waarop dat apparaat wordt gebruikt, inclusief maar niet beperkt tot: IP-adres, land en provider, merk en model van het apparaat, versie van het besturingssysteem van het apparaat, taalvoorkeur.

³ Applicatievoorkeuren zijn de instellingen in de mobiele applicatie die door een geautoriseerde gebruiker individueel zijn geconfigureerd, inclusief maar niet beperkt tot: Voorkeur voor pincode of Biometrische Snelle Login, Pushmeldingen (aan/uit), pushtokens (een token waarmee de mobiele telefoon van de geautoriseerde gebruiker gericht kan worden op pushmeldingen).

4. Doel van de verzamelde persoonsgegevens en wettelijke basis

De toepasselijke wetgeving inzake gegevensbescherming staat Nicolab toe uw persoonsgegevens te verwerken met het oog op de uitvoering van de diensten, zoals gedefinieerd in de relevante hoofdovereenkomst (uw werkgever) of op basis van uw toestemming.

5. Bewaartermijn van persoonsgegevens

De persoonsgegevens worden bewaard gedurende de tijd die nodig is voor de uitvoering, beëindiging of afloop van een hoofdovereenkomst en zodra onze wettelijke verplichtingen om gegevens te bewaren zijn verstreken. In de hoofdovereenkomst worden aanvullende bepalingen opgenomen over de duur van de gegevensopslag.

6. Subverwerking

6.1. Dienstverleners (verwerkers)

Om de goede werking van de diensten, waaronder de uitvoering van de hoofdovereenkomst, te garanderen, maakt Nicolab gebruik van externe diensten (zoals software van derden). Wij maken alleen gebruik van diensten die worden geleverd door dergelijke gegevensverwerkers die naar behoren kunnen garanderen dat passende technische en organisatorische maatregelen worden geïmplementeerd om ervoor te zorgen dat de verwerking van persoonsgegevens voldoet aan de vereisten van de toepasselijke wetgeving inzake gegevensbescherming en om de rechten te beschermen van de personen op wie de gegevens betrekking hebben. Voordat wij persoonsgegevens aan derden verstrekken, zullen wij een (sub)verwerkingsovereenkomst aangaan waarin wij hen passende beveiligingsnormen opleggen.

Nicolab maakt alleen persoonsgegevens openbaar als dit noodzakelijk is om een specifiek doel van de gegevensverwerking na te streven en alleen voor zover dit noodzakelijk is om een dergelijk doel te bereiken. Persoonsgegevens van de geautoriseerde gebruiker van onze diensten kunnen worden bekendgemaakt aan de dienstverleners om ons te voorzien van de technische, IT- en organisatorische oplossingen die Nicolab nodig heeft om zijn bedrijfsactiviteiten uit te voeren. Wij maken de persoonsgegevens van de geautoriseerde gebruiker alleen bekend aan een gecontracteerde leverancier als en voor zover dit noodzakelijk is om een specifiek doel van de gegevensverwerking hieronder te bereiken.

6.2. Andere ontvangers (verwerkingsverantwoordelijken)

Wij kunnen uw persoonsgegevens delen met de volgende verwerkingsverantwoordelijken (d.w.z. derde partijen die uw persoonsgegevens voor hun eigen doeleinden verwerken):

- wetshandhavings- of andere instanties als wij hiertoe wettelijk verplicht zijn, of door een bevelschrift, dagvaarding of gerechtelijk bevel om uw persoonsgegevens openbaar te maken.

7. Grensoverschrijdende gegevensoverdracht

De overdracht van persoonsgegevens die in het kader van de diensten worden verstrekt, voldoet aan de nationale en internationale wetgeving.

8. Rechten van de persoon op wie de persoonsgegevens betrekking hebben

U beschikt over de rechten op uw persoonsgegevens die hieronder worden beschreven.

- Recht op toegang, rectificatie, beperking, verwijdering of verplaatsing van persoonsgegevens. De persoon op wie de persoonsgegevens betrekking hebben, heeft het

recht om ons te verzoeken hem of haar toegang te verlenen tot zijn of haar persoonsgegevens, om dergelijke persoonsgegevens te corrigeren of te verwijderen ("het recht om vergeten te worden"), om de verwerking daarvan te beperken of er bezwaar tegen te maken, evenals om zijn of haar persoonsgegevens te laten verplaatsen.

- Recht om de toestemming op elk moment in te trekken. De persoon wiens Persoonsgegevens door Nicolab worden verwerkt op basis van de toestemming van een dergelijke persoon heeft op elk moment het recht om zijn of haar toestemming in te trekken, zonder dat dit invloed heeft op het recht om dergelijke persoonsgegevens te verwerken op basis van de toestemming voordat het werd ingetrokken.
- Recht om een klacht in te dienen. De persoon wiens persoonsgegevens door Nicolab worden verwerkt, heeft het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens, de Nederlandse toezichhoudende autoriteit.
- Recht om bezwaar te maken. De persoon wiens persoonsgegevens worden verwerkt, heeft het recht om op elk moment bezwaar te maken tegen de verwerking van zijn of haar persoonsgegevens.

U kunt uw rechten uitoefenen door contact met ons op te nemen via infosec@nicolab.com zodat wij uw verzoek kunnen beoordelen in overeenstemming met de toepasselijke wetgeving. Wanneer wij uw rechtenverzoek per e-mail ontvangen, aanvaardt u dat wij stappen kunnen ondernemen om uw identiteit te verifiëren voordat we aan het verzoek voldoen om uw privacy en veiligheid te beschermen, bijvoorbeeld door contact met u of uw werkgever op te nemen om uw identiteit en uw kwalificatie vast te stellen als een geautoriseerde gebruiker.

9. Beveiliging

Rekening houdend met de aard, reikwijdte, context en doeleinden van gegevensverwerking en het risico, hoe waarschijnlijk en dreigend ook, van schending van enig recht of vrijheid van natuurlijke personen, implementeert Nicolab passende technische en organisatorische maatregelen om de gegevensverwerking in overeenstemming te brengen met de toepasselijke wetgeving inzake gegevensbescherming en om dit te kunnen bewijzen. Onze beveiligingsmaatregelen worden voortdurend verbeterd naarmate de technologie zich ontwikkelt.

9.1. Technische maatregelen

Nicolab neemt technische maatregelen om te voorkomen dat onbevoegden elektronisch verzonden persoonsgegevens onderscheppen of wijzigen. Nicolab is ISO 27001 en ISO 13485 gecertificeerd.

9.2. Links naar externe websites

Onze diensten kunnen hyperlinks bevatten naar externe websites die niet door ons worden beheerd. Als u op een link van een derde partij klikt, wordt u naar de website van die derde partij geleid. Zodra u onze diensten heeft verlaten, kunnen wij niet verantwoordelijk zijn voor de bescherming en privacy van de informatie die u verstrekt. We raden u ten zeerste aan om het privacybeleid van Nicolab Services en de algemene voorwaarden van elke website die u bezoekt te lezen. Wij hebben geen controle over en aanvaarden geen verantwoordelijkheid voor de inhoud, het privacybeleid of de praktijken van websites, producten of diensten van derden.

9.3. Authenticatie en autorisatie van geautoriseerde gebruikers

De authenticatie van geautoriseerde gebruikers wordt volledig beheerd door het identiteitsprovidersysteem van het ziekenhuis, zoals een Active Directory File Server (ADFS). Op deze manier heeft het ziekenhuis volledige controle over het bepalen van het wachtwoordbeleid, welke

geautoriseerde gebruikers toegang hebben tot StrokeViewer, het afdwingen van meervoudige authenticatie, enz. Wanneer een geautoriseerde gebruiker dus probeert toegang te krijgen tot StrokeViewer, wordt deze geautoriseerde gebruiker doorgestuurd naar het identiteitsprovidersysteem van het ziekenhuis. Als het door het ziekenhuis gebruikte identiteitsprovidersysteem geen tweefactorauthenticatie ondersteunt, kan het ziekenhuis de StrokeViewer-app gebruiken om tweefactorauthenticatie te bieden.

Enmaal geauthenticeerd, is een geautoriseerde gebruiker geautoriseerd voor:

- 1 uur webtoegang tot het product;
- 336 uur (14 dagen) mobiele toegang tot het product.

Na het verstrijken van deze periode wordt de geautoriseerde gebruiker verzocht zich opnieuw te authenticeren. Ook worden de extra veiligheidsmaatregelen toegepast:

- als het geautoriseerde gebruikersaccount wordt opgeschort of ingetrokken door de identiteitsprovider van de klant, wordt de toegang tot het product automatisch beëindigd, uiterlijk binnen 1 uur;
- de mobiele app vereist dat de geautoriseerde gebruiker een extra pincode of biometrische gegevens verstrekt voor authenticatie;
- de webtoegang wordt automatisch vergrendeld na 20 minuten inactiviteit om ongeoorloofde toegang tot onbeheerde sessies te voorkomen. Om deze te ontgrendelen moet de geautoriseerde gebruiker zichzelf opnieuw authenticeren;
- als de geautoriseerde gebruiker naar een ander tabblad in de browser of naar een ander venster is overgeschakeld en gedurende 10 minuten niet terugkeert naar de webpagina van het product, wordt de webtoegang vergrendeld, zelfs als de geautoriseerde gebruiker met de andere applicaties en/of browsertabbladen blijft werken, om deze te ontgrendelen moet de geautoriseerde gebruiker zichzelf opnieuw authenticeren;
- mobiele toegang wordt automatisch vergrendeld na 1 minuut inactiviteit om ongeoorloofde toegang tot onbeheerde sessies te voorkomen. Om deze te ontgrendelen moet de geautoriseerde gebruiker een extra pincode of biometrie verstrekken.

10. Inbreuk op persoonsgegevens en meldplicht

In het geval van een inbreuk op de persoonsgegevens met betrekking tot de door Nicolab geleverde diensten, zal Nicolab de getroffen geautoriseerde gebruikers en, indien van toepassing, de relevante toezichthoudende autoriteiten, onmiddellijk op de hoogte stellen in het geval van een inbreuk op de persoonsgegevens die een risico vormt voor de rechten en vrijheden van de getroffen geautoriseerde gebruikers. De melding zal zonder onnodige vertraging worden gedaan nadat de inbreuk bekend is geworden, maar uiterlijk binnen 72 uur. In geval van een inbreuk op de persoonsgegevens zal Nicolab alle redelijke maatregelen nemen om de gevolgen van de inbreuk op de persoonsgegevens te beperken en/of een nieuwe voorkomen, tegen betaling van de redelijke kosten door u.

11. Wijzigingen in het privacybeleid van Nicolab Services

Nicolab behoudt zich het recht voor om dit privacybeleid van Nicolab Services op elk moment en naar eigen goeddunken te wijzigen, aan te passen of te veranderen. Dergelijke wijzigingen kunnen door Nicolab zonder voorafgaande kennisgeving worden doorgevoerd. Nicolab moedigt bezoekers aan om deze pagina regelmatig te controleren op de laatste informatie over onze privacypraktijken en op eventuele updates of herzieningen. Als u deze website blijft gebruiken na een wijziging in dit Nicolab Services Privacybeleid, betekent dit dat u een dergelijke wijziging accepteert.

Persoonlijke gegevensdetails

Beschrijving van diensten	<p>StrokeViewer is een Software as a Service (SaaS)-beeldverwerkingsapplicatie. StrokeViewer analyseert automatisch scans ontvangen van patiënten met symptomen van een beroerte. Na de analyse wordt een rapport gegenereerd met relevante kenmerken van de afbeeldingen voor beroerte. Deze functies kunnen door de arts worden gebruikt als ondersteunend hulpmiddel voor verdere diagnostiek.</p> <ol style="list-style-type: none"> 1. Automatische analyse van DICOM-afbeeldingen met behulp van StrokeViewer-algoritmen 2. Web DICOM-viewer, 3. Mobiele DICOM-viewer 4. Netwerkbreed delen van afbeeldingen 5. Instant messaging 6. Technische ondersteuning bij storingen of in andere gevallen wanneer dit noodzakelijk wordt geacht 7. Opleidingsdiensten
Type persoonsgegevens	1. Persoonsgegevens van geautoriseerde gebruikers met uitzondering van speciale categorieën persoonsgegevens (AVG Art.4,9)
Categorieën betrokkenen	1. Geautoriseerde gebruikers
Doeleinden van de verwerking	<p>Verwerking zal uitsluitend plaatsvinden in het kader van en voor de duur van de hoofdovereenkomst ten behoeve van:</p> <ul style="list-style-type: none"> - Dienstverlening - Communicatie - Diagnostiek en probleemoplossing - Personalisatie en maatwerk - Analyse en onderzoek - Wettelijke naleving
Goedgekeurd Verwerkers	Google Cloud, Stream.io
Bewaar termijn	1. Het logbestand wordt bewaard zolang het contract met klant loopt, maar niet langer dan 5 jaar