

Datenschutzrichtlinie für Nicolab-Dienste

Zuletzt geändert am 06.03.2024

1. Einführung

Nicolab respektiert Ihre Privatsphäre in Bezug auf alle Informationen, die wir bei der Erbringung unserer Dienstleistungen sammeln. Personenbezogene Daten sind Informationen, mit denen Sie oder andere Personen direkt oder indirekt identifiziert werden können („personenbezogene Daten“), wie z. B. Vorname, Nachname oder E-Mail-Adresse.

Wir geben Ihre personenbezogenen Daten nicht an Dritte weiter, außer an unsere verbundenen Unternehmen und Datenverarbeiter, die uns bei der Erbringung unserer Dienstleistungen unterstützen, oder an Behörden, wenn wir zur Einhaltung von Gesetzen oder Gerichtsbeschlüssen dazu verpflichtet sind. Mit Ihrer Einwilligung verwenden wir Cookies für Marketing-, Leistungs- und Statistikzwecke.

Sie haben jederzeit das Recht unentgeltlich Auskunft über Ihre gespeicherten personenbezogenen Daten, deren Herkunft und Empfänger sowie den Zweck ihrer Erhebung zu verlangen. Ferner haben Sie das Recht, die Berichtigung, Sperrung oder Löschung der Daten zu verlangen. Sie können sich jederzeit unter der nachfolgend genannten Adresse unseres Datenschutzbeauftragten an uns wenden, wenn Sie weitere Fragen zum Thema Privatsphäre und Datenschutz haben. Selbstverständlich können Sie auch eine Beschwerde bei den zuständigen Aufsichtsbehörden einreichen.

2. Allgemeine Bestimmungen

Diese Datenschutzrichtlinie für Nicolab-Dienste gilt für personenbezogene Daten, die von Nicolab (im Folgenden „uns“, „wir“) im Zusammenhang mit dem Betrieb und den Diensten verarbeitet werden, die wir Ihnen über unsere Abonnementdienste, die StrokeViewer-App und die Website (nicolab.com) (zusammenfassend als „Dienste“ bezeichnet) anbieten. In dieser Datenschutzrichtlinie für Nicolab-Dienste wird erläutert, welche personenbezogenen Daten gesammelt werden können, wie wir sie verwenden, wie Sie Ihre Rechte ausüben können und unter welchen Umständen wir diese personenbezogenen Daten an Dritte weitergeben können. Wir verarbeiten auch Patientendaten im Auftrag Ihrer Organisation, wofür wir eine separate Datenverarbeitungsvereinbarung mit Ihrer Organisation abgeschlossen haben.

Personenbezogene Daten werden von NICo-Lab B.V. verwaltet, eingetragen im Handelsregister der Handelskammer in Amsterdam unter der Registrierungsnummer (KvK): 64531775, mit Hauptgeschäftssitz und Zustellanschrift unter Paasheuvelweg 25, 1105 BP, Amsterdam, Niederlande.

Nicolab hat einen Datenschutzbeauftragten ernannt, der unter folgender Adresse kontaktiert werden kann: infosec@nicolab.com.

Wir verarbeiten Ihre personenbezogenen Daten, um Ihnen unter anderem folgende Dienstleistungen¹ bereitzustellen zu können:

- Automatische Analyse von DICOM-Bildern mithilfe von StrokeViewer-Algorithmen
- Web-DICOM-Viewer
- Mobiler DICOM-Viewer

¹ Die vollständige Liste der Dienste ist in der Hauptvereinbarung enthalten und kann für die jeweilige Partei unterschiedlich sein.

- Netzwerkweite Weitergabe von Bildmaterial
- Instant-Messaging
- Technischer Support bei Störungen oder in anderen Fällen, wenn dies als notwendig erachtet wird
- Schulungsdienste

Personenbezogene Daten, die im Zusammenhang mit den Diensten übermittelt werden, werden in Übereinstimmung mit den geltenden Datenschutzgesetzen verarbeitet.

Durch die Nutzung unserer Dienste erklären Sie sich mit der Verarbeitung Ihrer personenbezogenen Daten gemäß den in dieser Datenschutzrichtlinie für Nicolab-Dienste festgelegten Bedingungen einverstanden.

Darüber hinaus regelt eine separate Vereinbarung zwischen uns und unserem Kunden die Bereitstellung, den Zugriff und die Nutzung der Dienste (die „Hauptvereinbarung“), einschließlich der Verarbeitung personenbezogener Daten, Dateien oder anderer Inhalte, die bei der Nutzung der Dienste übermittelt werden (zusammenfassend als „Kundendaten“ bezeichnet). Die Organisation (z. B. Ihr Arbeitgeber oder eine andere Stelle oder Einzelperson), die den Hauptvertrag abgeschlossen hat („Kunde“), kontrolliert bestimmte Aspekte ihrer Nutzung der Dienste (ihre „Anwendung“) und der damit verbundenen Kundendaten, z. B. wie lange Nicolab Kundendaten speichert.

Soweit die Verarbeitung Ihrer personenbezogenen Daten auf der Grundlage Ihrer Einwilligung erfolgt, werden wir den Umfang dieser Verarbeitung nicht ändern, es sei denn, Sie haben eine zusätzliche Einwilligung für einen solchen geänderten Umfang der Verarbeitung erteilt.

Wenn Sie als Mitarbeiter eines Kunden tätig sind, legt diese Datenschutzrichtlinie für Nicolab-Dienste zusammen mit der Hauptvereinbarung die Bestimmungen und Richtlinien für Ihre Nutzung unserer Dienste fest.

3. Umfang der erhobenen und verarbeiteten personenbezogenen Daten

Wir können die folgenden personenbezogenen Daten im Rahmen unseres Hauptvertrags oder der Gewährung des Zugangs von Einzelpersonen zu einer Anwendung von Nicolab verarbeiten („autorisierte Benutzer“). Darüber hinaus können wir Daten über die Einstellungen der Anwendung selbst erheben, z. B. über die Benachrichtigungseinstellungen und die bevorzugte Anmeldemethode.

Personenbezogene Daten von autorisierten Benutzern, die gesammelt werden, um autorisierten Benutzern die Nutzung der Dienste zu ermöglichen:

1. Im Rahmen der Leistungserbringung erhobene Daten:
 - Vollständiger Name
 - Berufsbezeichnung
 - Arbeitgeber
 - E-Mail-Adresse
 - Mobiltelefonnummer (optional)
 - IP-Adresse
 - Sitzungscookies

2. Daten, die im Falle eines Zugriffs auf die Dienste über ein mobiles Endgerät erhoben werden:
 - Profil des Mobilgerätes²
 - Anwendungspräferenzen³
 - Anwendungs-PIN-Code (optional)

3. Im Rahmen des Instant-Messaging-Dienstes erfasste Daten:
 - Übermittelte Texte und Medien

Auf StrokeViewer kann über einen Browser oder eine mobile Anwendung mit der länderspezifischen Domain StrokeViewer.com zugegriffen werden (z. B. in den Niederlanden nl.strokeviewer.com).

Autorisierte Benutzer müssen vor der Nutzung der Dienste eine Schulung absolvieren. Die Schulungsinhalte können sich je nach Aufgabenbereich des autorisierten Benutzers unterscheiden, und Informationen zur Schulung werden per E-Mail mitgeteilt.

Nicolab bietet Unterstützung bei technischen Problemen im Zusammenhang mit der Nutzung der Dienste. Wenn der Support-Desk kontaktiert wird, können die folgenden Details erfasst werden, um das Problem besser lösen zu können.

Zusätzliche Daten:

- Protokolldaten: Wie bei den meisten über das Internet bereitgestellten Technologiediensten sammeln unsere Server automatisch Informationen, wenn Sie auf unsere Dienste zugreifen oder diese nutzen, und speichern diese in Protokolldateien.
- Kundendaten: Die Bereitstellungen sind so konfiguriert, dass sie Kundendaten an Nicolab senden, um die Dienste zu nutzen. So können beispielsweise digitale Computertomographie-Untersuchungen (CT) über die Dienste an Nicolab gesendet werden, damit ein Algorithmus mit künstlicher Intelligenz verdächtige Befunde wie einen Großgefäßverschluss erkennen kann. Zu den Kundendaten können auch Gesundheitsdaten gehören. Solche sensiblen Daten erfordern ein höheres Maß an Schutz. Wir benötigen eine umfassendere Grundlage für die Erhebung, Speicherung und Nutzung dieser Art personenbezogener Daten. Solche sensiblen Daten unterliegen der Hauptvereinbarung und der Datenverarbeitungsvereinbarung zwischen dem Kunden und Nicolab und nicht dieser Datenschutzrichtlinie für Nicolab-Dienste.

Aufgrund unseres berechtigten Interesses können wir Ihre E-Mail-Adresse auch dazu verwenden, Ihnen Post-Market-Umfragen zuzusenden. Wenn Sie die Nutzung Ihrer E-Mail-Adresse zu diesem Zweck nicht wünschen, können Sie dieser Verarbeitung jederzeit widersprechen.

² Beim Mobilgeräteprofil handelt es sich um die Sammlung einer Vielzahl von Daten über das Gerät eines autorisierten Benutzers und die Art und Weise, wie dieses Gerät verwendet wird, wie z. B. IP-Adresse, Land und Netzbetreiber, Gerätemarke und -modell, Version des Betriebssystems des Geräts und Spracheinstellung.

³ Anwendungspräferenzen sind die von einem autorisierten Benutzer individuell konfigurierten Einstellungen in der mobilen Anwendung, wie z. B. Bevorzugung eines Pincodes oder einer biometrischen Schnellanmeldung, Push-Benachrichtigungen (ein/aus), Push-Token (ein Token, der es ermöglicht, das Mobiltelefon des autorisierten Benutzers für Push-Benachrichtigungen zu aktivieren).

4. Zweck der erhobenen personenbezogenen Daten und Rechtsgrundlage

Die geltenden Datenschutzgesetze erlauben es Nicolab, Ihre personenbezogenen Daten zum Zweck der Erbringung der Dienstleistungen gemäß der Definition in der jeweiligen Hauptvereinbarung (mit Ihrem Arbeitgeber) oder auf der Grundlage Ihrer Einwilligung zu verarbeiten.

5. Aufbewahrungsfrist personenbezogener Daten

Die personenbezogenen Daten werden so lange gespeichert, wie es für die Durchführung, die Beendigung oder das Auslaufen einer Hauptvereinbarung erforderlich ist, und werden gelöscht, sobald unsere gesetzlichen Aufbewahrungspflichten erloschen sind. Weitere Bestimmungen über die Dauer der Datenspeicherung sind in der Hauptvereinbarung enthalten.

6. Auftragsverarbeitung

6.1. Dienstleister (Auftragsverarbeiter)

Um das ordnungsgemäße Funktionieren der Dienste, einschließlich der Erfüllung der Hauptvereinbarung, sicherzustellen, nutzt Nicolab externe Dienste (z. B. Software von Drittanbietern). Wir nutzen nur Dienste von solchen Datenverarbeitern, die ordnungsgemäß garantieren können, dass geeignete technische und organisatorische Maßnahmen umgesetzt werden, um die Übereinstimmung der Verarbeitung personenbezogener Daten mit den Anforderungen der geltenden Datenschutzgesetze sicherzustellen und die Rechte der Personen zu schützen, auf die sich die Daten beziehen. Bevor wir personenbezogene Daten an Dritte weitergeben, schließen wir eine Auftragsverarbeitungsvereinbarung ab, die ihnen angemessene Sicherheitsstandards auferlegt.

Nicolab gibt personenbezogene Daten nur dann weiter, wenn dies zur Verfolgung eines bestimmten Zwecks der Datenverarbeitung erforderlich ist, und nur insoweit, wie es zur Erfüllung eines solchen Zwecks notwendig ist. Personenbezogene Daten des autorisierten Benutzers unserer Dienste können an die Dienstleister weitergegeben werden, um uns die technischen, IT- und organisatorischen Lösungen bereitzustellen, die Nicolab für die Ausübung seiner Geschäftstätigkeit benötigt. Wir geben die Personenbezogenen Daten des autorisierten Benutzers nur dann an einen beauftragten Anbieter weiter, wenn und soweit dies zur Erfüllung eines bestimmten Zwecks der Datenverarbeitung nach diesem Vertrag erforderlich ist.

6.2. Weitere Empfänger (Verantwortliche)

Wir können Ihre personenbezogenen Daten an die folgenden Verantwortlichen weitergeben (d. h. Dritte, die Ihre personenbezogenen Daten für ihre eigenen Zwecke verarbeiten):

- Strafverfolgungsbehörden oder andere Behörden, wenn wir gesetzlich dazu verpflichtet sind oder aufgrund eines Haftbefehls, einer Vorladung oder eines Gerichtsbeschlusses Ihre personenbezogenen Daten offenlegen müssen.

7. Grenzüberschreitende Datenübertragung

Die Übermittlung personenbezogener Daten im Rahmen der Dienste erfolgt im Einklang mit nationaler und internationaler Gesetzgebung.

8. Rechte der Person, auf die sich die personenbezogenen Daten beziehen

Sie haben die im Folgenden beschriebenen Rechte in Bezug auf Ihre personenbezogenen Daten.

- Recht auf Zugang, Berichtigung, Einschränkung, Löschung oder Übertragung personenbezogener Daten – die Person, auf die sich die personenbezogenen Daten

beziehen, hat das Recht, von uns Zugang zu ihren personenbezogenen Daten zu verlangen, diese zu berichtigen oder zu löschen („Recht auf Vergessenwerden“), ihre Verarbeitung einzuschränken oder ihr zu widersprechen sowie die Übertragung ihrer personenbezogenen Daten zu veranlassen.

- Recht auf jederzeitigen Widerruf der Einwilligung – die Person, deren personenbezogene Daten von Nicolab auf der Grundlage ihrer Einwilligung verarbeitet werden, hat das Recht, ihre Einwilligung jederzeit zu widerrufen, ohne dass dadurch das Recht berührt wird, die vor dem Widerruf erteilten personenbezogenen Daten auf der Grundlage der Einwilligung zu verarbeiten.
- Recht, eine Beschwerde einzureichen – die Person, deren personenbezogene Daten von Nicolab verarbeitet werden, ist berechtigt, eine Beschwerde bei der niederländischen Aufsichtsbehörde („Autoriteit Persoonsgegevens“) einzureichen.
- Recht auf Widerspruch – die Person, deren personenbezogene Daten verarbeitet werden, ist berechtigt, jederzeit Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen.

Sie können Ihre Rechte ausüben, indem Sie uns unter infosec@nicolab.com kontaktieren, damit wir Ihre Anfrage in Übereinstimmung mit dem geltenden Recht prüfen können. Wenn wir Ihre Anfrage zur Ausübung von Rechten per E-Mail erhalten, erklären Sie sich damit einverstanden, dass wir zum Schutz Ihrer Privatsphäre und Ihrer Sicherheit Maßnahmen zur Überprüfung Ihrer Identität ergreifen können, bevor wir der Anfrage nachkommen, z. B. indem wir uns mit Ihnen oder Ihrem Arbeitgeber in Verbindung setzen, um Ihre Identität und Ihre Qualifikation als autorisierter Nutzer festzustellen.

9. Sicherheit

In Anbetracht der Art, des Umfangs, der Rahmenbedingungen und der Zwecke der Datenverarbeitung sowie des Risikos einer Verletzung von Rechten oder Freiheiten natürlicher Personen, und ungeachtet der Wahrscheinlichkeit einer solchen Verletzung, ergreift Nicolab geeignete technische und organisatorische Maßnahmen, um die Datenverarbeitung mit den geltenden Datenschutzgesetzen in Einklang zu bringen und dies nachweisen zu können. Unsere Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert.

9.1. Technische Maßnahmen

Nicolab ergreift technische Maßnahmen, um zu verhindern, dass Unbefugte elektronisch übermittelte personenbezogene Daten abfangen oder verändern. Nicolab ist nach ISO 27001 und ISO 13485 zertifiziert.

9.2. Links zu externen Seiten

Unsere Dienste können Hyperlinks zu externen Websites enthalten, die nicht von uns betrieben werden. Wenn Sie auf einen Link eines Drittanbieters klicken, werden Sie zur Website dieses Drittanbieters weitergeleitet. Wenn Sie den Bereich unserer Dienste erst einmal verlassen haben, tragen wir keine Verantwortung mehr für den Schutz und die Geheimhaltung der von Ihnen bereitgestellten Informationen. Wir raten Ihnen dringend, die jeweiligen allgemeinen Geschäftsbedingungen besuchter Websites auf etwaige Unterschiede zur Datenschutzrichtlinie für Nicolab-Dienste zu prüfen. Wir haben keine Kontrolle über die Inhalte, Datenschutzrichtlinien oder Praktiken von Websites, Produkten oder Dienstleistungen Dritter und übernehmen keine Verantwortung dafür.

9.3. Authentifizierung und Autorisierung autorisierter Benutzer

Die Authentifizierung der autorisierten Benutzer wird vollständig vom Identitätsmanagementsystem des Krankenhauses verwaltet, z. B. einem Active Directory File Server (ADFS). Somit hat das Krankenhaus die

vollständige Kontrolle über die Festlegung von Passwortrichtlinien, welche autorisierten Benutzer Zugang zu StrokeViewer erhalten, die Durchsetzung der Multi-Faktor-Authentifizierung usw. Wenn also ein autorisierter Benutzer versucht, auf StrokeViewer zuzugreifen, wird dieser autorisierte Benutzer an das Identitätsmanagementsystem des Krankenhauses weitergeleitet. Wenn das vom Krankenhaus verwendete Identitätsmanagementsystem keine Zwei-Faktor-Authentifizierung unterstützt, kann das Krankenhaus die StrokeViewer-App verwenden, um eine Zwei-Faktor-Authentifizierung zu ermöglichen.

Nach der Authentifizierung erhält ein autorisierter Benutzer folgende Berechtigungen:

- 1 Stunde Webzugriff auf das Produkt;
- 336 Stunden (14 Tage) mobiler Zugriff auf das Produkt.

Nach Ablauf dieser Fristen wird der autorisierte Benutzer aufgefordert, sich erneut zu authentifizieren. Die zusätzlichen Sicherheitsmaßnahmen werden ebenfalls angewendet:

- Wenn das Konto des autorisierten Benutzers vom Identitätsmanagementsystem des Kunden gesperrt oder widerrufen wird, wird sein Zugriff auf das Produkt spätestens nach einer Stunde automatisch beendet.
- Die mobile App erfordert, dass der autorisierte Benutzer eine zusätzliche PIN oder biometrische Daten zur Authentifizierung bereitstellt.
- Der Webzugriff wird nach 20 Minuten Inaktivität automatisch gesperrt, um unbefugten Zugriff auf unbeaufsichtigte Sitzungen zu verhindern. Zum Entsperren muss sich der autorisierte Benutzer erneut authentifizieren.
- Wenn der autorisierte Benutzer in seinem Browser zu einer anderen Registerkarte oder zu einem anderen Fenster wechselt und innerhalb von 10 Minuten nicht zur Produkt-Webseite zurückkehrt, wird sein Webzugang gesperrt, auch wenn der autorisierte Benutzer weiterhin mit anderen Anwendungen und/oder Browser-Registerkarten arbeitet; um ihn zu entsperren, muss sich der autorisierte Benutzer erneut authentifizieren;
- Der mobile Zugriff wird nach einer Minute Inaktivität automatisch gesperrt, um unbefugten Zugriff auf unbeaufsichtigte Sitzungen zu verhindern. Zum Entsperren muss der autorisierte Benutzer eine zusätzliche PIN oder biometrische Daten angeben.

10. Verletzung des Schutzes personenbezogener Daten und Meldepflicht

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den von Nicolab erbrachten Diensten wird Nicolab die betroffenen berechtigten Nutzer und ggf. die zuständigen Aufsichtsbehörden unverzüglich benachrichtigen, falls die Verletzung personenbezogener Daten ein Risiko für die Rechte und Freiheiten der betroffenen autorisierten Nutzer darstellt. Die Meldung hat unverzüglich nach Bekanntwerden der Verletzung zu erfolgen, spätestens jedoch innerhalb von 72 Stunden. Im Falle einer Verletzung des Schutzes personenbezogener Daten wird Nicolab alle angemessenen Maßnahmen ergreifen, um die Folgen der Verletzung des Schutzes personenbezogener Daten zu begrenzen und/oder eine erneute Verletzung zu verhindern, und zwar gegen Übernahme der angemessenen Kosten durch Sie.

11. Änderungen der Datenschutzrichtlinie für Nicolab-Dienste

Nicolab behält sich das Recht vor, diese Datenschutzrichtlinie für Nicolab-Dienste jederzeit und nach eigenem Ermessen zu ändern, zu ergänzen oder anzupassen. Solche Änderungen können von Nicolab ohne vorherige Ankündigung vorgenommen werden. Nicolab empfiehlt Besuchern, diese Seite regelmäßig zu besuchen, um die neuesten Informationen zu unseren Datenschutzpraktiken sowie

Aktualisierungen oder Überarbeitungen zu erhalten. Durch Ihre fortgesetzte Nutzung dieser Website nach einer Änderung dieser Datenschutzrichtlinie für Nicolab-Dienste erklären Sie sich mit dieser Änderung einverstanden.

Angaben zu personenbezogenen Daten

Beschreibung der Dienste	<p>StrokeViewer ist eine SaaS-Bildverarbeitungsanwendung (Software as a Service). StrokeViewer analysiert auf automatische Weise die Scans von Patienten mit Schlaganfallsymptomen. Nach der Analyse wird ein Bericht erstellt, der relevante Merkmale der Bilder für Schlaganfälle enthält. Dieser Funktionsumfang kann vom Arzt als Hilfsmittel für eine weitere Diagnostik genutzt werden.</p> <ol style="list-style-type: none"> 1. Automatische Analyse von DICOM-Bildern mithilfe von StrokeViewer-Algorithmen 2. Web-DICOM-Viewer, 3. Mobiler DICOM-Viewer 4. Netzwerkweite Weitergabe von Bildmaterial 5. Instant-Messaging 6. Technischer Support bei Störungen oder in anderen Fällen, wenn dies als notwendig erachtet wird 7. Schulungsdienste
Art der personenbezogenen Daten	1. Personenbezogene Daten von autorisierten Benutzern, mit Ausnahme besonderer Kategorien von personenbezogenen Daten (DSGVO Art. 4,9)
Kategorien der Betroffenen	1. Autorisierte Benutzer
Zwecke der Verarbeitung	<p>Die Verarbeitung erfolgt nur im Rahmen und für die Dauer der Hauptvereinbarung zu folgenden Zwecken:</p> <ul style="list-style-type: none"> - Bereitstellung von Diensten - Kommunikation - Diagnose und Fehlerbehebung - Personalisierung und Individualisierung - Analytik und Forschung - Einhaltung gesetzlicher Vorschriften
Zugelassene Verarbeiter	Google Cloud, Stream.io, Mixpanel
Aufbewahrungsfrist	1. Die erfassten Protokolldaten werden so lange aufbewahrt, wie der Vertrag mit dem Kunden gültig ist, jedoch nicht länger als 5 Jahre.