FAQ – Datenschutz und -sicherheit bei neolexon Aphasie im Klinik-Einsatz

1. **Können wir einen Auftragsverarbeitungsvertrag (AV) abschließen?**
   Ja, wir bieten allen Nutzern einen AV an entsprechend den gesetzlichen Anforderungen aus Art. 28 DSGVO. Dieser ist zum Download HIER bereitgestellt und bereits von uns unterzeichnet. Laden Sie das Dokument bitte herunter und zeichnen es ebenfalls. Anschließend schicken Sie es an info@neolexon.de. Herzlichen Dank.

   Sollte Ihre Klinik lediglich einen eigenen AV anwenden wollen, werden wir diesen prüfen und ggf. unterzeichnen.

2. **Können Sie Zertifikate zur Datensicherheit und Informationssicherheit bereitstellen?**
   Unser Unternehmen hat ein umfassendes Informationssicherheits-Managementsystem (ISMS) etabliert und ist nach ISO 27001 zertifiziert. Das Zertifikat ist HIER abzurufen. Wir bestätigen, dass wir die Anforderungen aus § 393 SGB V erfüllen. Unsere Anwendung wird ausschließlich in der Open Telekom Cloud in Deutschland gehostet, die über ein gültiges C5-Testat (Typ 2) verfügt. Dieses können wir Ihnen auf Anfrage zur Verfügung stellen. Zudem setzen wir die im Testat beschriebenen korrespondierenden Kriterien für Kunden (Complementary User Entity Controls, CUECs) gemäß § 393 Abs. 3 Nr. 3 SGB V vollständig um. Richten Sie hierzu Ihre Anfrage bitte an datenschutz@neolexon.de.

3. **Ist neolexon Aphasie ein Medizinprodukt?**
   Ja, es handelt sich um ein Medizinprodukt Klasse I nach MDR

4. **Liegt ein Handbuch zur App vor?**
   Ja, wir bieten eine Gebrauchsanweisung für die Therapeuten Aphasie-App und für die Patienten Aphasie-App an.

5. **Liegt eine Systembeschreibung vor?**
   Eine gesonderte Systembeschreibung liegt nicht vor. Bitte sehen Sie unsere Gebrauchsanweisungen (Therapeuten-App, Aphasie-App für Patienten) ein.

6. **Liegt eine Datenschutzfolgenabschätzung vor?**
   Ja, eine DSFA wird in regelmäßigen Abständen zusammen mit unserem Datenschutzbeauftragten durchgeführt entsprechend den Anforderungen aus Art. 35 DSGVO. Im Zuge dessen werden auch die Positivlisten der Datenschutzbehörden regelmäßig evaluiert und etwaige Datenschutzrisiken evaluiert bzw. behandelt. Einschlägige Risiken, die eine vorherige Konsultation nach Art. 36 DSGVO erfordern, liegen bis dato nicht vor.

7. **Liegt ein Rollen- und Berechtigungskonzept vor?**
   Ja, ein Rollen- und Berechtigungskonzept liegt vor. Die vorliegende Dokumentation und deren Umsetzungen erfüllen neben Anforderungen des Datenschutzes auch solche der Datensicherheit und Informationssicherheit. Wir orientieren uns hierbei an Standards wie dem Erforderlichkeitsprinzip (engl. Need-to-Know) und Prinzip der geringsten Berechtigung (engl. Least Privilege).

8. **Liegt ein Löschkonzept vor?**

Ja, ein Löschkonzept liegt vor, das ebenfalls mit dem Datenschutzbeauftragten abgestimmt und regelmäßig evaluiert wird. Dieses beinhaltet unter anderem folgende Löschvorgänge:

- Supportanfragen werden nach Abschluss des Supportfalles gelöscht,
- Nutzeraccounts können von neolexon Nutzern selbstständig oder per Anfrage vollständig gelöscht werden,
- nach Ende der Nutzung der DiGA neolexon Aphasie (Patienten Eigentraining zuhause) wird der Nutzeraccount automatisch gelöscht,
- angelegte Patienten-Profile im Therapeuten-Account können durch Therapeut:innen selbstständig gelöscht werden,
- beim Löschen der App vom Endgerät werden alle zugehörigen Daten vollständig vom Endgerät gelöscht.
- Daten, die unter gesetzliche Aufbewahrungsfristen fallen, etwa Rechnungsdokumente, werden entsprechend der gesetzlichen Anforderungen aufbewahrt

9. Kann die Datenschutzfolgenabschätzung, das Rollen- und Berechtigungskonzept und das Löschkonzept ausgehändigt werden?

Wir möchten Ihnen an dieser Stelle, neben der vertraglichen Verpflichtung, nochmals versichern, dass wir unser datenschutzrechtliches Pflichtenheft aus Art. 28 DSGVO sowie Art. 32 DSGVO ernst nehmen. Eine unmittelbare Zusendung der nachfolgenden, internen Dokumente ist allerdings nicht davon erfasst:

- Datenschutzfolgenabschätzung
- Rollen- und Berechtigungskonzept
- Löschkonzept bzw. -richtlinie

Die vertraglichen Verpflichtungen stellen sicher, dass alle Maßnahmen gemäß Art. 32 DSGVO getroffen und nachgewiesen werden, u.a. auch durch Nachweisdokumente wie ein ISO 27001 Zertifikat. Weiterhin kommen wir allen Unterstützungsleistungen gemäß Art. 28 Abs. 3 lit. f DSGVO nach, indem wir eng mit unseren Auftraggebern zusammenarbeiten. Demgemäß stellen wir etwa auf Nachfrage alle einschlägigen Informationen bereit, damit Verantwortliche bei Bedarf eine eigene Datenschutzfolgenabschätzung durchführen können. Die Übersendung der entsprechenden, internen Dokumente ist nicht zuletzt aus Datenschutz- und Datensicherheitsgründen nicht möglich, da die Dokumente vertrauenswürdige Angaben zu unserem Unternehmen und Rollen- bzw. Personalstrukturen enthalten.

10. Werden bei neolexon Aphasie personenbezogene Daten der Patient:innen verarbeitet?

Ja, bei der Registrierung als neolexon Patient:in (Patienten-Account für Nutzung der Patient:innen App für zuhause) werden durch die Patient:innen folgende Daten angegeben:
E-Mail-Adresse, Vor- und Nachname, Passwort.

Ja, wenn Therapeut:innen in ihrem Account neue Patienten-Profile anlegen und Patient:innen in der Therapeuten-App oder im Eigentraining üben, werden folgende Daten erhoben:

- Optional: Vor- und Nachname der Patient:innen, Geschlecht, Diagnose
- Dauer des Trainings
- individuelles Übungsmaterial und Schwierigkeitseinstellungen
- individuelle Leistung

11. **Aufgrund welcher Voraussetzung werden die personenbezogenen Daten der Patient:innen durch Therapeut:innen eingegeben?**
    Limedix stellt eine Schweigepflichtsentbindung zur Verfügung, die Patient:innen unterzeichnen und Therapierende bei sich ablegen.

12. **Wer erstellt die Patienten-Profile?**
    Der/die behandelnde Sprachtherapeut:in.

13. **Können Patient:innen auch pseudonymisiert in der App angelegt werden?**
    Ja, dies ist möglich. Therapeut:innen können die Patienten-Profile auch pseudonymisiert erstellen, z.B. nur mit einer Patient:innen-Nummer oder den Initialen der Patient:innen.

14. **Werden Beschäftigtendaten verarbeitet?**
    Zur Registrierung wird eine von Nutzer:innen bestimmte E-Mail-Adresse verwendet. Hier kann auch eine unpersönliche E-Mail-Adresse von Nutzer:innen verwendet werden, z.B. Sprachtherapie@klinik.de.
    Des Weiteren kann bei der Registrierung in das Feld Vor- und Nachname im Falle einer Klinik entweder der Name der Klinik, des/der Ansprechpartner:in im Therapeut:innen-Team oder einfach "Abteilung Logopädie" eingegeben werden. Dies ist den jeweiligen Nutzer:innen überlassen.
    Wir erheben außerdem die IP-Adresse vom Endgerät der Klinik, mit der sich Nutzer:innen in unsere App einloggen.
    Falls durch Beschäftigte der Klinik eine Support-Anfrage an uns gestellt wird, werden hier ebenfalls die E-Mail-Adresse des Absenders erfasst und für die Dauer des Support-Falls im E-Mail-Postfach des Support-Teams gespeichert.

    Ansonsten erheben und verarbeiten wir keine Angaben zu Beschäftigten.

15. **Welche Statistiken werden erfasst?**
    - Dauer des Trainings
    - individuelles Übungsmaterial und Schwierigkeitseinstellungen
    - individuelle Leistung, d.h. Anzahl der Fehler und korrekt geösten Aufgaben innerhalb der Übungen auf Einzelitem-Ebene und aggregiert über Übungstypen und unterschiedliche Zeiträume

16. **Ist Datenminimierung sichergestellt?**
    Ja, wir folgen dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO. Wir stellen somit sicher, dass alle Verarbeitungen personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind.

17. **Werden alle Grundsätze der DSGVO sichergestellt?**
    Ja, wir befolgen alle Grundsätze der DSGVO gemäß Art. 5 DSGVO: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; Zweckbindung; Datenminimierung; Richtigkeit; Speicherbegrenzung; Integrität und Vertraulichkeit; Rechenschaftspflicht

18. **Erfolgt eine Datenübermittlung an externe Empfänger? Wenn ja, an welche?**
    Wir übermitteln Daten lediglich an die von uns geprüften, vertraglich verpflichteten Dienstleister (Auftragsverarbeitung), die zur Bereitstellung des Angebots erforderlich

sind. Hierbei handelt es sich insbesondere um die Deutsche Telekom, die infrastrukturelle Dienstleistungen zum Hosting in Deutschland bereitstellt. Die von uns beauftragten Dienstleister können dem gemeinsamen Auftragsverarbeitungsvertrag entnommen werden.

19. **Findet die Datenspeicherung/Datenverarbeitung ausschließlich in der Europäischen Union statt?**
    Ja, wir legen großen Wert auf ein Hosting und eine Datenverarbeitung innerhalb der Europäischen Union. Die maßgebliche, von uns genutzte Infrastruktur der Deutschen Telekom befindet sich in Deutschland.

20. **Haben Patient:innen die Möglichkeit, die App zu Hause zu nutzen?**
    Die Klinik-Version und Praxis-Version der Aphasie-App sind für das Üben in der Therapiestunde und für das Eigentraining während des Klinik-Aufenthaltes auf dem Endgerät der Klinik.

    Wenn Patient:innen zuhause Üben möchten, kann die Patient:innen-Version der neolexon Aphasie- App genutzt werden. Die DiGA kann bei Entlassung rezeptiert werden.

21. **Wird zur Nutzung der App ein Internetzugriff benötigt?**
    Ja, eine Internetverbindung ist für folgende Schritte notwendig:
    - Installation der App aus dem Apple App Store oder Google Playstore auf dem Endgerät
    - Im Falle der Nutzung der Browser-Version der App, durchgehende Internetverbindung nötig
    - Im Falle der Nutzung auf dem Tablet ist Internet zum Login, Erstellen neuer Patienten-Profile, Zusammenstellung neuer Übungs-Materialsets, Download der Materialsets auf das Tablet. Zum Durchführen der Übungen ist hingegen kein Internet notwendig.

22. **Benötigt Limedix eine Fernwartungsmöglichkeit?**
    Nein

23. **Wird Cloud-Computing genutzt?**
    Ja, die Datenspeicherung und Datenverarbeitung erfolgt auf Servern der Deutschen Telekom innerhalb Deutschlands. Wir legen großen Wert auf Hosting in Deutschland, um rechtliche Datenschutzrisiken zu vermeiden und Vertrauen zu schaffen.

24. **Werden mobile Geräte genutzt? Welche Betriebssysteme werden unterstützt?**
    Die neolexon Aphasie-App kann über den Browser am Laptop/PC oder nach Installation auf Android oder iOS Tablets genutzt werden. Die technischen Herausforderungen für die Endgeräte können HIER eingesehen werden.

25. **Wird künstliche Intelligenz eingesetzt?**
    Nein.

26. **Gibt es eine:n Ansprechpartner:in für Klinik-Kunden?**
    Ja, Kathrin Leicht, k.leicht@neolexon.de, Tel: 089 24886-4442

27. **Besteht die Möglichkeit einen Testzugang für die benötigte kostenpflichtige Version zu erhalten?**
    Ja, wir bieten allen Nutzern nach der Registrierung eine 14-tägige kostenlose Testphase. Falls eine längere Testphase benötigt wird, wenden Sie sich bitte an unsere Ansprechpartnerin für Kliniken k.leicht@neolexon.de

28. **Kann eine Einweisung in das Medizinprodukt erfolgen?**
    Wir bieten eine persönliche Einweisung in einer online Produktvorstellung für das Therapeut:innen-Team an. Eine Bestätigung über die erfolgte Einweisung können wir gerne ausstellen.

    Es steht zudem eine kostenlose Telefonnummer für Rückfragen zur Verfügung, sodass alle Nutzer:innen jederzeit Fragen stellen können. Sie erreichen unseren geschulten Kundensupport von Montag - Freitag zwischen 8 und 15 Uhr unter der Telefonnummer 089 24886 4440.

29. **Unterstützt die Anwendung eine zwei Faktor Authentifizierung (2FA)?**
    Nein

30. **Kann die Anwendung so konfiguriert werden, dass nach einer definierten Zeit eine neuerliche Anmeldung notwendig wird?**
    Ja

31. **Kann in der Klinik-Version der App verhindert werden, dass Patient:innen auf die Ansicht der Therapeut:innen zugreifen?**
    Ja, in der Klinik-Version kann ein Sperrmuster festgelegt werden, das verhindert, dass Patient:innen, die auf dem Gerät der Klinik das Eigentraining nutzen, auf die Bedienoberfläche der Therapeut:innen zugreifen kann.

32. **Finden regelmäßige Updates statt? Wenn ja, wie wird darüber informiert?**
    Ja, es finden regelmäßige Updates statt. Es wird empfohlen diese zeitnah zu installieren, bzw. die automatische Update-Installation zu aktivieren. Über Updates mit Funktionserweiterungen oder sicherheitsrelevante Updates wird über den Newsletter und per Popup direkt in den Apps informiert. Alle Updates werden während eines gebuchten Lizenzzeitraums kostenfrei bereitgestellt.