Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Praxis/Klinik

_____

_____

_____

-im Folgenden: **Auftraggeber**-

und

Limedix GmbH
Sendlinger Straße 2
80331 München

-im Folgenden: **Limedix**-

Der Auftraggeber (für die Verarbeitung verantwortlich) und Limedix schließen den folgenden Vertrag zur Auftragsverarbeitung gemäß Art. 28 der europäischen Datenschutz-Grundverordnung (DSGVO). Auf Grundlage des zwischen den Parteien bestehenden Vertragsverhältnisses (Hauptvertrag) verarbeitet Limedix personenbezogene Daten für den Auftraggeber. Die sich daraus ergebenden datenschutzrechtlichen Rechte und Verpflichtungen der Parteien werden durch diesen Auftragsverarbeitungsvertrag konkretisiert. Die Anlagen zu diesem Vertrag sind Bestandteil der Vereinbarung. Die getroffenen Regelungen finden Anwendung auf alle Leistungen, welche Limedix für den Auftraggeber erbringt und sämtliche damit verbundenen Tätigkeiten, welche eine Verarbeitung personenbezogener Daten zur Folge haben und zur Folge haben können.

§ 1 Gegenstand und Dauer der Verarbeitung

a) Gegenstand des Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch Limedix für den Auftraggeber in dessen Auftrag und nach dessen Weisung. Der Gegenstand und die Dauer des Vertrages richten sich nach dem Hauptvertrag.
b) Limedix stellt ein EDV-System für die Sprachtherapie bereit. Damit können Patientenprofile erstellt und individuelles Übungsmaterial aus einer Datenbank ausgewählt werden. Das Übungsmaterial wird zum Üben auf Endgeräte des Auftraggebers und ggf. der Patienten übertragen. Im Anschluss werden ggf. individuelle Statistiken erstellt, die den Übungserfolg des Patienten darstellen.
c) Limedix erhebt und verarbeitet dabei personenbezogene Daten im Auftrag des Auftraggebers nach Art. 28 DSGVO. Die Rahmenbedingungen der Verarbeitung dieser Daten als Auftragnehmer werden im Folgenden festgelegt.

§ 2 Umfang, Art und Zweck der Verarbeitung

- Erstellung von Patientenprofilen in der Web-App, der Browser-App und in den mobilen Apps
- Erstellung von individuellem Übungsmaterial für Patienten in der Web-App, der Browser-App und den mobilen Apps
- Übertragung des individuellen Übungsmaterials zwischen den Apps
- Erfassen von Statistiken in den Apps
- Übertragung der Statistiken zwischen den Apps

- Visualisierung von Statistiken in den Apps
- Einstellen der Übungsschwierigkeit für Patienten in der Web-App, Browser-App und den mobilen Apps

§ 3 Art der personenbezogenen Daten

Limedix erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. der Auftraggeber erlaubt Limedix folgende personenbezogene Daten zu erheben:

- optional: Patientenname, Geschlecht, Geburtsdatum, Diagnose
- individuelles Übungsmaterial und Schwierigkeitseinstellungen
- individuelle Statistiken und Erfolgskontrolle

§ 4 Kreis der betroffenen Personen

Bei den betroffenen Personen der oben aufgelisteten Daten handelt es sich um:

- Patienten des Auftraggebers

§ 5 Rechte und Pflichten des Auftraggebers, Kontrollrechte

a) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und somit Verantwortlicher im Sinne des Art. 4 Abs. 7 DSGVO.

b) Der Auftraggeber erteilt Limedix Weisungen über die Art und den Umfang der Verarbeitung der personenbezogenen Daten.

c) Vor Beginn des Auftrages und der damit verbundenen Datenverarbeitung und im Anschluss regelmäßig ist der Auftraggeber berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten, sich von der Einhaltung der bei Limedix getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen.

d) Limedix erklärt sich damit einverstanden, dass sich der Auftraggeber jederzeit nach vorheriger Ankündigung von der Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte überzeugen kann, dies insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Systeme sowie sonstige Kontrollen vor Ort. Dem Auftragnehmer im Rahmen von Kontrollen entstehende Kosten und Aufwendungen, soweit sie über die Anforderungen der DSGVO hinausgehen, erstattet der Auftraggeber.

e) Limedix hat eventuelle Kontrollmaßnahmen der Datenschutzaufsichtsbehörde gem. Art. 58 DSGVO und § 40 BDSG-neu zu dulden. Er wird den Auftraggeber unverzüglich nach Ankündigung oder Kenntniserlangung über die Durchführung der Kontrollmaßnahme sowie bei anderweitigen Anfragen, Ermittlungen oder Erkundigungen der Datenschutzaufsichtsbehörde, insbesondere auch, wenn diese im Rahmen einer vorherigen Konsultation gem. Art. 36 DSGVO erfolgen, informieren, soweit die Maßnahmen oder Anfragen Datenverarbeitungen betreffen können, die Limedix für den Auftraggeber erbringt.

f) Auf Verlangen des Auftraggebers weist Limedix die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis durch die Vorlage eines aktuellen Testats oder Berichts (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder einem externen Datenschutzauditor) und gegebenenfalls einer geeigneten Zertifizierung (z.B. nach BSI-Grundschutz, ISO27001 oder nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO) oder die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO erbracht werden. Die Kontrollrechte des Auftraggebers bleiben hiervon unberührt.

§ 6 Pflichten von Limedix

a) Limedix ist verpflichtet, personenbezogene Daten ausschließlich weisungsgemäß und nach den Vorgaben dieses Vertrages zu verarbeiten.

b) Bei der Gewährung der Rechte der Betroffenen gemäß Art. 15 ff. DSGVO (Berichtigung, Einschränkung der Verarbeitung, Löschung, Benachrichtigung und Auskunftserteilung) wird Limedix den Auftraggeber auf erstes Anfordern im Rahmen seiner Möglichkeiten unterstützen. Limedix wird hierfür geeignete technische und organisatorische Maßnahmen treffen. Limedix hat auf Weisung die personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken.

c) Sollte die im Auftrag des Auftraggebers erhobenen Daten Gegenstand eines Verlangens auf Datenportabilität gemäß Art. 20 DSGVO sein, wird Limedix dem Auftraggeber den betreffenden Datensatz unverzüglich auf Anforderung in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

d) Sofern sich eine betroffene Person unmittelbar an Limedix mit der Wahrnehmung ihrer Betroffenenrechte wendet, hat dieser dieses Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.

e) Limedix wird den Auftraggeber unverzüglich darauf hinweisen, wenn dieser der Meinung ist, dass eine erteilte Weisung gegen gesetzliche Vorschriften verstößt. Die Durchführung der entsprechenden Weisung kann dieser solange aussetzen, bis sie durch den Auftraggeber bestätigt oder abgeändert wird.

f) Limedix stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und anderen für Limedix tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet Limedix, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort. Sofern Limedix im Zusammenhang mit den Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis gemäß dem Telekommunikationsgesetz zu verpflichten.

g) Limedix bestätigt, dass er, sofern die Voraussetzungen dafür vorliegen, gemäß Art. 37 DSGVO einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht. Externer Datenschutzbeauftragter von Limedix ist Frank Trautwein, dsb@freshcompliance.de, Tel.: 030 92148707.

§ 7 Leistungsort

a) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung durch den Auftraggeber und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

b) Sofern die Verarbeitung personenbezogener Daten außerhalb der EU erfolgt, garantiert Limedix, dass die nach den jeweils geltenden Datenschutzvorschriften anwendbaren Voraussetzungen für das Eingreifen eines Erlaubnistatbestandes für die Verarbeitung personenbezogener Daten außerhalb der EU erfüllt sind ("datenschutzrechtliche Rechtfertigung"). Dies ist zum einen gegeben, sofern und soweit die EU-Kommission diesem bzw. dieser ein angemessenes Schutzniveau bescheinigt hat. Weiterhin wenn die Verarbeitung der personenbezogenen Daten außerhalb der EU ausschließlich im Rahmen geeigneter Garantien erfolgt, die ebenfalls ein angemessenes Schutzniveau sicherstellen. Hierfür erfolgt ein Rückgriff auf Standardvertragsklauseln der EU-Kommission in Verbindung mit einer einzelfallbezogenen Evaluation zusammen mit dem Datenschutzbeauftragten. Die Standardvertragsklauseln dienen der vertraglichen Sicherstellung und des Nachweises, dass die Verarbeitung personenbezogener Daten außerhalb der EU die Vorgaben des europäischen Datenschutzrechts erfüllen.

§ 8 Unterauftragsverhältnisse

a) Unterauftragsverhältnisse bedürfen in jedem Einzelfall der vorherigen schriftlichen Zustimmung des Auftraggebers. Die Zustimmungspflicht gilt auch für die Beauftragung von weiteren Auftragsverarbeitern, die ihren Sitz außerhalb des Europäischen Wirtschaftsraumes haben und somit nicht unter Art. 28 DSGVO fallen.

b) Limedix ist für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich. Limedix wird den Namen, die Anschrift und das Tätigkeitsfeld, sowie den Vertragszweck schriftlich oder in Textform dem Auftraggeber mitteilen. Limedix wird außerdem schriftlich oder in Textform versichern, dass er den weiteren Auftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat und er sich von den beim weiteren Auftragsverarbeiter eingesetzten technischen und organisatorischen Maßnahmen überzeugt hat. Der Auftraggeber hat das Recht sich selbst von der Eignung der weiteren Auftragsverarbeitern zu überzeugen. Limedix wird dem Auftraggeber auf Anfrage eine Kopie des Unterauftragsverarbeitungsvertrages zur Verfügung stellen.

c) Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Limedix bleibt jedoch zu jeder Zeit verantwortlich für jegliche Handlung oder Unterlassung der von ihm beauftragten weiteren Auftragsverarbeitern, in selber Weise wie er für die eigenen Handlungen und Unterlassungen verantwortlich ist.

d) Limedix hat die Einhaltung der Pflichten des weiteren Auftragsverarbeiters regelmäßig zu überprüfen. Limedix hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der weitere Auftragsverarbeiter die zugesicherten und erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

e) Limedix arbeitet derzeit bei der Erfüllung des Auftrags mit dem folgenden weiteren Auftragsverarbeiter zusammen, mit dessen Beauftragung sich der Auftraggeber einverstanden erklärt:

Name und Anschrift des Subunternehmers	Beschreibung der Leistungen
1. Telekom Cloud, T-Systems International GmbH, Hahnstr. 43d, 60528 Frankfurt am Main, Germany	Cloud-basierte Infrastruktur (IaaS)

f) Kommt bei einem künftig geplanten neuen Subunternehmer-Einsatz keine Einigung zustande, besteht für beide Seiten ein außerordentliches Kündigungsrecht für den zugrundeliegenden Dienstleistungsvertrag sowie diese Vereinbarung.

§ 9 Technische und organisatorische Maßnahmen

a) Limedix ist verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung gem. Art 32 i.V.m Art. 5 Abs. 1 DSGVO einzuhalten. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen, mit denen eine angemessene Pseudonymisierung und Verschlüsselung gewährleistet werden kann sowie Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten.

b) Die von Limedix getroffenen technischen und organisatorischen Maßnahmen sind ausführlich in der Anlage zu diesem Vertrag dargestellt und sind Vertragsbestandteil.

§ 10 Haftung

a) Limedix haftet gegenüber dem Auftraggeber gemäß der gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diesen Vertrag, sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die Limedix, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Die Haftung für leichte Fahrlässigkeit ist ausgeschlossen.

b) Für den Ersatz von Schäden, die ein Betroffener aufgrund einer nach der DSGVO oder dem BDSG-neu oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses geltend macht, ist der Auftraggeber bzw. Limedix gem. Art. 82 DSGVO gegenüber dem Betroffenen verantwortlich. Limedix stellt den Auftraggeber im Innenverhältnis von allen Schadensersatzansprüchen frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus diesem Vertrag durch Limedix gegen den Auftraggeber geltend gemacht werden.

§ 11 Schlussbestimmungen

a) Dem Auftraggeber ist bekannt, dass neben dem Datengeheimnis gegebenenfalls auch das Privat- bzw. Patientengeheimnis zu beachten ist. Der Auftraggeber sichert Limedix zu, diesen Geheimnissen unterliegende Informationen nur zugänglich zu machen, sofern er hierfür vom Betroffenen von der Verschwiegenheitspflicht entbunden wurde.

b) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

c) Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

d) Sollte eine Bestimmung dieser Vereinbarung unwirksam oder nicht durchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Die unwirksame oder nicht durchsetzbare Bestimmung ist durch eine wirksame und durchsetzbare Bestimmung zu ersetzen, welche dem Zweck der ersetzenden Bestimmung am nächsten kommt.

e) Diese Vereinbarung unterliegt deutschem Recht.

f) Sofern der Zugriff auf die Daten durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat Limedix den Auftraggeber unverzüglich hierüber zu benachrichtigen.

_____	München, 01.04.2021
Ort, Datum	Ort, Datum
_____	
Auftraggeber	Limedix GmbH

ANLAGE - Technische und organisatorische Maßnahmen

Limedix speichert keine Informationen des Auftraggebers auf lokalen Systemen. Zur Speicherung und Verarbeitung der Daten des Auftraggebers wird die Telekom Cloud verwendet. Die Produkte und Services der Telekom Cloud (T-Systems International GmbH) sind DSGVO- und BDSG-neu-konform. Alle Datencenter der Telekom Cloud sind ausschließlich in Deutschland verortet. Darüber hinaus sind sie ISO 27017, ISO 27108, CSA Star Level 2, TÜV Trusted Cloud, ISO 27001, ISO 20000, ISO 90001, ISO 22301, ISO 14001 und Cloud TCDP Version 1.0 zertifiziert. Besonders mit TCDP Version 1.0 als primärer Standard wird die Datensicherheit in der Cloud sichergestellt und die Verpflichtung zur Privatsphäre und zum Schutz personenbezogener Daten bewiesen.

Limedix versichert gemeinsam mit seiner Infrastruktur als Service (IaaS) der Telekom Cloud die folgenden technischen und organisatorischen Maßnahmen getroffen zu haben:

1. Maßnahmen zur Sicherung der Vertraulichkeit

a) Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren.

Beschreibung des Zutrittskontrollsystems (Limedix):

- kontrollierte Schlüsselvergabe
- Türsicherung (elektronischer Türöffner, etc.)
- Überwachungseinrichtung
- verschlossener Aktenschrank

Beschreibung des Zutrittskontrollsystems (Telekom Cloud):

- Festlegung von Sicherheitsbereichen
- Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen
- Begleitung von Besuchern und Fremdpersonal
- Überwachung der Räume außerhalb der Betriebszeiten
- Protokollierung des Zutritts zu den datenverarbeitenden IT Systemen

b) Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems (Limedix):

- starker SSH-Schlüssel basierter Zugriff mit Verwendung von Zwei-Faktor-Authentisierung
- automatische Zugangssperre bei Inaktivität
- Einrichtung eines Benutzerstammsatzes pro User
- Explizite Bestimmung und Begrenzung der Zahl der berechtigten Mitarbeiter
- Verschlüsselung von Datenträgern
- Access-Listen
- Abkapselung von sensiblen Systemen durch getrennte Netzbereiche
- Authentifizierungsverfahren
- Protokollierung der Anmeldeversuche

Beschreibung des Zugangskontrollsystems (Telekom Cloud):

- Zugangsschutz (Authentisierung)
- starke Authentisierung bei höchstem Schutzniveau
- einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
- gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk
- Personen mit Zugangsberechtigung werden explizit bestimmt und auf ein Minimum beschränkt
- personengebundene Authentifizierungsmedien werden dokumentiert und verwaltet
- Protokollierung der erfolgreichen und abgewiesenen Zugangsversuche
- Festlegung befugter Personen
- automatische und manuelle Zugangssperre bei Verlassen des Arbeitsplatzes

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden

personenbezogenen Daten zugreifen können, sodass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems (Limedix):

- Berechtigungskonzepte (Profile, Rollen, etc.) und deren Dokumentation
- Auswertung/Protokollierungen
- Verschlüsselung von unterschiedlichen Datenträgern
- Archivierungskonzept
- Autorisierungstests
- Umsetzen von Zugriffsbeschränkungen

Beschreibung des Zugriffkontrollsystems (Telekom Cloud):

- Erstellen eines Berechtigungskonzepts
- Umsetzen von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Personengebundene Zugriffberechtigungen werden verwaltet und dokumentiert
- Protokollierung des Datenzugriffs

d) Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs (Limedix):

- Berechtigungskonzepte
- verschlüsselte Speicherung von personenbezogenen Daten
- Softwareseitige Kundentrennung
- Trennung von Test- und Produktivsystemen

e) Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung des Pseudonymisierungsverfahrens (Limedix):

- Speicherung der Nutzeridentität in einem Stammdatensatz auf einer verschlüsselten Festplatte. Andere Daten können ohne Assoziierung mit dem Stammdatensatz nicht identifiziert werden.

2. Maßnahmen zur Sicherung der Integrität

a) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Beschreibung der Weitergabekontrolle (Limedix):

- Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen
- Transportprozesse mit individueller Verantwortlichkeit
- Verschlüsselungsverfahren, die Datenveränderungen während des Transports aufdecken

Beschreibung der Weitergabekontrolle (Telekom Cloud):

- Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl
- sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sicherheitsgateways an den Netzübergabepunkten
- Löschung voreingestellter Dienstkonten/Passwörter und nicht benötigter Dienste
- Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
- Jede Maschine die in das IV-Verfahren einbezogen ist, besitzt eine eindeutige Kennung/Passwort
- Die Datenspeicherung erfolgt ausschließlich auf der Plattform und dem Backup-System
- Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit Kundendaten des Auftraggebers wird protokolliert

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Beschreibung des Eingabekontrollvorgangs (Limedix):

- Protokollierung sicherheitsrelevanter Systemaktivitäten und Aufbewahrung dieser Protokolle von mindestens 1 Monat
- Protokollierung wann und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind

3. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems (Limedix):

- Datensicherungsverfahren (stündliche Backups)
- Spiegeln der Daten in zwei verschiedenen geographisch redundanten Datencentern (Geographische Verfügbarkeitszonen)

- Spiegeln der Daten in mehreren Datenbankservern
- Automatischer Serverneustart und Einspringen der Backup Server

Beschreibung des Verfügbarkeitskontrollsystems (Telekom Cloud):
- Unterbrechungsfreie Stromversorgung
- Brandmeldeanlage
- Klimaanlage
- Alarmanlage
- Notfallplan
- keine wasserführenden Leitungen über oder neben Serverräumen

b) rasche Widerherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen (Limedix):
- Datensicherungsverfahren (stündliche Backups)
- regelmäßige Tests der Datenwiederherstellung

4. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren (Limedix):
- Datenschutzmanagement
- Formalisierte Prozesse für Datenschutzvorfälle
- Weisungen des Auftraggebers werden dokumentiert
- formalisiertes Auftragsmanagement
- Service-Level-Agreements für die Durchführung von Kontrollen