VIROMED MEDICAL

VitaLab

Vereinbarung zur Auftragsverarbeitung
Artikel 28 DSGVO

Version 2.1 / Stand: 27.10.2021

Inhalt

1. Vertragsgegenstand 3
2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Dauer der Auftragsverarbeitung 3
3. Weisungsrechte des Auftraggebers 3
4. Pflichten des Auftraggebers 4
5. Pflichten des Auftragnehmers 4
6. Sicherheit der Verarbeitung 5
7. Kontrollrechte des Auftraggebers 5
8. Unterauftragsverhältnisse 6
9. Übermittlung von Auftraggeber-Daten an Drittländer 7
10. Rückgabe und Löschung von Auftraggeber-Daten 7
11. Laufzeit und Kündigung 7
12. Vorrangklausel 7
13. Anlagen: 7

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen 8

Anlage 2: Technische und organisatorische Maßnahmen 9

Anlage 3: Unterauftragnehmer 13

1. Vertragsgegenstand

Im Rahmen des zwischen den Parteien bestehenden Liefer- und Leistungsverhältnisses (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO ist (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Dauer der Auftragsverarbeitung

Der Auftragnehmer verarbeitet die personenbezogenen Daten während der Dauer des Hauptvertrages im Auftrag und nur nach Weisung des Auftraggebers. Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen werden in **Anlage 1** festgelegt. Jede davon abweichende oder darüber hinaus gehende Verarbeitung von personenbezogenen Daten, insbesondere zu eigenen Zwecken, ist dem Auftragnehmer untersagt.

3. Weisungsrechte des Auftraggebers

3.1 Die Weisungen des Auftraggebers erfolgen grundsätzlich in Schrift- oder Textform (z.B. E-Mail). Abweichend hiervon können (fern-) mündliche Weisungen erfolgen, die im Nachgang in Schrift- bzw. Textform bestätigt werden.

3.2 Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich oder ggf. unter Einhaltung einer durch den Auftraggeber festgelegten, angemessenen Frist auszuführen und insbesondere personenbezogene Daten auf Weisung des Auftraggebers unverzüglich zu berichtigen, zu löschen oder zu sperren und dies auf Verlangen schriftlich zu bestätigen.

3.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag, gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen.

3.4 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber den Grund der Verarbeitung und die entsprechenden rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist nach außen, also gegenüber Dritten und den Betroffenen, für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

4.2 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen (insbesondere in Bezug auf technische und organisatorische Maßnahmen der Datensicherheit) des Auftragnehmers vertraulich zu behandeln. Dieser Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4.3 Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

5. Pflichten des Auftragnehmers

5.1 Soweit sich eine betroffene Person in Wahrnehmung ihrer Rechte aus Kapitel 3 DSGVO (Art. 12 bis 23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32 bis 37 BDSG) unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt den Auftraggeber auf zumutbare Weise mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung solcher Anträge auf Wahrnehmung der in Kapitel 3 DSGVO benannten Rechte der betroffenen Person nachzukommen.

5.2 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

5.3 Wenn dem Auftragnehmer hinsichtlich der verarbeiteten Auftraggeber-Daten eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt wird („Datenschutzvorfall“), meldet er dies dem Verantwortlichen unverzüglich. Im Rahmen der Meldung gem. Art. 33 Abs. 2 DSGVO teilt der Auftragnehmer dem Auftraggeber nach Möglichkeit den Zeitpunkt sowie Art und Ausmaß des Vorfalls, das betroffene IT-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die daraufhin ergriffenen Maßnahmen mit.

5.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn Rechte des Auftraggebers an den personenbezogenen Daten beim Auftragnehmer durch Maßnahmen Dritter oder durch sonstige Ereignisse maßgeblich berührt werden.

5.5 Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers sämtliche Auftraggeber-Daten herauszugeben. Vom Auftraggeber erhaltene Datenträger sind gesondert zu kennzeichnen und laufend zu verwalten. Kopien und Duplikate der personenbezogenen Daten dürfen ausschließlich nach vorheriger Zustimmung durch den Auftraggeber angefertigt werden, sofern sie nicht zur

ordnungsgemäßen Durchführung dieser Vereinbarung bzw. des jeweiligen Projektauftrags oder zur Einhaltung von gesetzlichen Aufbewahrungspflichten dienen.

5.6 Sofern eine gesetzliche Pflicht besteht, benennt der Auftragnehmer einen Datenschutzbeauftragten (Art. 37 ff. DSGVO) und teilt dessen Kontaktdaten sowie ggf. den Wechsel des Datenschutzbeauftragten dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mindestens in Textform mit.

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen insbesondere die Fähigkeit ein, die Vertraulichkeit, die Integrität, die Verfügbarkeit sowie der Belastbarkeit der Systeme auf Dauer sicherzustellen und die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Der Auftragnehmer führt regelmäßig eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch und dokumentiert die Ergebnisse.

6.2 Der Auftragnehmer garantiert, dass er vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen implementiert, während der Dauer der Verarbeitung aufrechterhält und wenn erforderlich dem Stand der Technik und dem Risiko der Verarbeitung anpassen wird.

6.3. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.4. Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die einem Berufsgeheimnis i.S. des § 203 Strafgesetzbuch (StGB) unterliegen. Der Auftragnehmer gewährleistet, sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Verschwiegenheit gem. § 203 Ab. 4 verpflichtet haben.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftragnehmer räumt dem Auftraggeber ein Kontrollrecht zur Prüfung der Datenverarbeitung sowie Einhaltung dieses Vertrags bzw. des jeweiligen Projektauftrags ein. Insbesondere stellt der Auftragnehmer dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht die Durchführung von Überprüfungen einschließlich Inspektionen. Die Kontrollhandlungen können ebenfalls durch einen zur Geheimhaltung verpflichteten Dritten vorgenommen werden, sofern es sich bei dem Dritten um keinen Konkurrenten des Auftragnehmers handelt.

7.2 Die Parteien sind sich einig, dass der Auftraggeber eine Überprüfung nach Ziffer 7.1 durchführt, indem er den Auftragnehmer anweist, nach seiner Wahl ein geeignetes Testat, einen Bericht oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditor oder Qualitätsauditor) oder eine geeignete

Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001 oder BSI-Grundschutz – („Prüfungsbericht“) vorzulegen. In begründeten Ausnahmen kann der Auftraggeber eigenständige Inspektionen durchführen.

7.3 Der Auftragnehmer verpflichtet sich, die Durchführung der Kontrollen zu unterstützen. Dies beinhaltet die Gewährung sämtlicher benötigter Zugangs-, Auskunfts- und Einsichtsrechte. Gleiches gilt für öffentliche Kontrollen durch die zuständige Aufsichtsbehörde gemäß den anwendbaren Datenschutzvorschriften.

7.4 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8. Unterauftragsverhältnisse

8.1 Der Auftragnehmer darf Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern (Subdienstleister) begründen. Zurzeit beschäftigt der Auftragnehmer die in **Anlage 3** bezeichneten Subdienstleister. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subdienstleistern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innerhalb von zwei Wochen Einspruch zu erheben, wobei dies nicht ohne wichtigen datenschutzrechtlichen Grund erfolgen darf. Sofern der Auftraggeber keine begründeten Einwände innerhalb von 2 Wochen ab Mitteilung über die Änderung erhebt, gilt diese als durch den Auftraggeber genehmigt. Der Auftragnehmer weist den Auftraggeber bei Beginn der Frist auf diese Bedeutung seines Verhaltens hin. Im Fall eines Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtige Änderung für den Auftragnehmer nicht zumutbar ist – die Leistung gegenüber dem Auftraggeber innerhalb von zwei Wochen nach Zugang des Einspruchs einstellen und den Hauptvertrag fristlos und mit sofortiger Wirkung kündigen.

8.2 Ist die Beauftragung eines Subdienstleisters mit einer Übermittlung der Auftraggeber-Daten in ein Land außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraum (EWR) („Drittland“) verbunden, gelten zusätzlich die Vorgaben aus Ziffer 9.

8.3 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Datenschutzpflichten, auch gegenüber dem Subdienstleister gelten und diesen gem. Art. 28 Abs. 4 DSGVO vor Aufnahme der Tätigkeiten entsprechend im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zu verpflichten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

9. Übermittlung von Auftraggeber-Daten an Drittländer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Übermittlung der Auftraggeber-Daten in ein Land außerhalb von EU/EWR („Drittland“) erfolgt nur wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

10. Rückgabe und Löschung von Auftraggeber-Daten

10.1 Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Abschluss der Erbringung der Verarbeitungsleistungen und insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) an den Auftraggeber herauszugeben und anschließend datenschutzgerecht zu löschen (inkl. vorhandener Kopien). Von dem Auftraggeber erhaltene Datenträger sind an den Auftraggeber zurückzugeben oder unter Einhaltung einer angemessenen Schutzstufe zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

10.2 Dokumentationen und Protokolle, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Laufzeit und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

12. Vorrangklausel

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

13. Anlagen

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen
Anlage 2: Technische und organisatorische Maßnahmen
Anlage 3: Unterauftragnehmer

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Art und Zweck der Datenverarbeitung:

Bei der Datenverarbeitung handelt es sich um die Zurverfügungstellung von erstellten Laborergebnissen und Immunitätsstatus an die betroffene Person.

Art der personenbezogenen Daten:

Personenbezogene Daten (Anrede, Geschlecht, Name, Nachname, Geburtsdatum, Adresse, Handynummer, Festnetznummer, E-Mail-Adresse, Krankenversicherungsdaten), besonders sensible personenbezogene Daten wie Gesundheitsdaten (insb. Immunitätsstatus und Labortestergebnisse), berufliche Organisationsdaten (Adress- und Kontaktdaten des Auftraggebers) berufliche Kontaktdaten (Mitarbeiter: Name, Vorname, Geschlecht, E-Mail-Adresse, Telefonnummer, Mobilnummer)

Kategorien betroffener Personen:

Auftraggeber und Mitarbeiter des Auftraggebers, Kunden des Auftraggebers (Jede Person, mit der eine Kunden-Geschäftsbeziehung besteht, z.B. private Personen, Pflegepatienten), Jede natürliche Person, mit der eine Geschäftsbeziehung besteht (mit dem Auftraggeber) außer Kunden; z.B. Inhaber und Mitarbeiter von Pflegeeinrichtungen, Ärzte, Praxismitarbeiter, Testzentrum. Kinder (Personen unter 16 Jahren; z.B. als Patienten)

Anlage 2: Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Die Büroräume sind mit Sicherheitsschlössern ausgestattet, für welche nur wenige ausgewählte Mitarbeiter Schlüssel besitzen. Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. Alarmanlage, Chipkarten/Transpondersysteme, Schließsystem mit Codesperre, Videoüberwachung der Eingänge und sämtlicher kritischer Gebäudeteile, Schlüsselregelung, Besucherbuch/Protokoll der Besucher, Sorgfalt bei der Auswahl der Reinigungsdienste

Zugangskontrolle/Verschlüsselung

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Zugang zu Daten rollenbasiert gesichert. Zugang zu Produktivdaten nur für eingeschränkte Nutzerzahl möglich. - Zugang zu extern gehosteten/betriebenen IT-Systemen ist besonders gesichert (Verschlüsselung, VPN) - Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall) - Zugang zu IT-Systemen nur mit Benutzerkennung und individuellem Passwort möglich - Passwortrichtlinie wird über Active Directory durchgesetzt. - IT-Systeme werden bei wiederholt erfolglosem Anmeldeversuch automatisch gesperrt. - Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit - Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. Anti-Viren-Software Server, Firewall, Intrusion Detection Systeme, Einsatz von VPN bei Remote-Zugriffen, Verschlüsselung von Notebooks, allg. Richtlinie Datenschutz und-sicherheit.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer, zentrale Verwaltung und Steuerung - Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt. - Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen. - Aufzeichnung von Zugriffen auf das IT-System - Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. physische Löschung von Datenträgern, Protokollierung von Zugriffenauf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten, Einsatz von Berechtigungskonzepten, minimale Anzahl an Administratoren, Verwaltung der Benutzerrechte durch Administratoren.

Trennungskontrolle/Zweckbindungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Trennung der Zugriffsregelungen über Datenbankprinzip
- Softwareseitige Mandantentrennung
- Trennung von Produktiv- und Testsystemen (in getrennten Datenbanken)
- Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. Trennung von Produktiv- und Testumgebung, physikalische Trennung (Systeme/Datenbanken/Datenträger), Steuerung über Berechtigungskonzept, Datensätze mit Zweckattributen versehen.

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung, VPN).
- Wiederbeschreibbare Datenträger werden vor der Wiederverwendung nach Standard DOD 5220-220.M gelöscht.
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.
- Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. Email-Verschlüsselung, Einsatz von VPN, Bereitstellung über verschlüsselte Verbindungen wie sftp, https, Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen.

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung
- Protokollierung gescheiterter Zugriffsversuche
- Protokollierung aller Aktivitäten auf dem Server
- Sicherung der Protokolldaten gegen Verlust oder Veränderung
- Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. technische Protokollierung der Eingabe, Änderung und Löschung von Daten, Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können, Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

- Datensicherheitskonzept
- Versionierte Daten- und Systembackups nach Backup-Plan (täglich/wöchentlich)
- Festplattenspiegelung (RAID), Backup-Rechenzentrum
- Schadsoftwareschutz
- Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
- Erhaltene und auszuliefernde Datenträger werden Schadsoftwarecheck unterzogen.
- Notfallplan
- Unterbrechungsfreie Stromversorgung
- Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. Feuer- und Rauchmeldeanlagen, Feuerlöscher Serverraum, Serverraumüberwachung von Temperatur und Feuchtigkeit, Serverraumklimatisierung, Backup- & Recovery-Konzept (ausformuliert), regelm. Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse, getrennte Partitionen für Betriebssysteme und Daten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

- Auftragnehmer werden sorgfältig ausgesucht.
- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten.
- Für die Verarbeitung von Behandlungsdaten von Patienten werden nur die Windcloud 4.0 GmbH als Cloud-Anbieter und Trilion s.r.l. als Softwareentwickler (freier Mitarbeiter) in Anspruch genommen.
- Ärzte werden über neue Verdachtsfälle mittels E-Mail (Microsoft) oder -wenn keine E-Mail-Adresse hinterlegt wurde- per Fax (Teamnet GmbH, retarus GmbH) benachrichtigt. Dabei werden keine Klarnamen, sondern nur pseudonymisierte Daten übermittelt (s. Anlage 2, Punkt 5. Pseudonymisierung).
- Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation, sorgfältige Auswahl des Auftragsnehmers, bei längerer Zusammenarbeit laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Datenschutz-Management

Maßnahmen, die eine Steuerung der Datenschutzprozesse ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherstellen:

- Es wurde eine fachkundige Person zum Datenschutzbeauftragten benannt:
David Oberbeck, E-Mail: datenschutzbeauftragter@vitabook.de
- Es gibt ein dokumentiertes Datenschutz-Management-System.
- Beschäftigte werden regelmäßig im Datenschutz geschult und sensibilisiert und sind über die Vertraulichkeit von Daten belehrt.
- Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung, Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundgesetz oder ISIS12, Datenschutzbeauftragter: dsgvoNORD GmbH, Erfüllung der Informationspflichten nach Art. 13 und 14

DSGVO

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- Personenbezogene Patienten- und Behandlungsdaten werden im ILD-board nach Möglichkeit automatisch pseudonymisiert (Extrahierung der Initialen aus Vor- und Nachname des Patienten). - Hochgeladene Dokumente (dicom oder Bilddateien, pdf-Dokumente) können nicht oder nur bedingt durch den Auftragnehmer automatisch pseudonymisiert werden. - Bei der Übermittlung von Nachrichten an Ärzte per E-Mail oder Fax werden keine Klarnamen übermittelt, sondern nur pseudonymisierte Daten. Dem Arzt selbst ermöglicht diese Pseudonymisierung dennoch eine vereinfachte Zuordnung der Behandlungsfälle. - Wir nehmen IT Hosting/Cloud-Dienste der windcloud 4.0 GmbH in Anspruch, welche umfassende Maßnahmen gewährleistet; dies sind u.a. im Falle einer Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System, interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren.

Anlage 3: Unterauftragnehmer

Name	Anschrift/Land	Auftragsinhalt
Windcloud 4.0 GmbH	Lecker Straße 7, 25917 Enge-Sande	Cloud Service
Microsoft Ireland Operations Ltd	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18, P521, Ireland	MS Outlook, MS Teams
Trilion Tech, s.r.o.	Fialková 2528/13, 955 01 Topol'cany, Slowakei	Softwareentwicklungsleistungen
Teamnet GmbH	Technologiepark 20 33100 Paderborn	Faxdienste

Viromed Medical GmbH
Flensburger Straße 18
25421 Pinneberg

Geschäftsführer Christoph Schostek
Eingetragen beim Amtsgericht
Pinneberg HRB 15638
USt. DE33 73 89 529

Telefon 040 – 429347077
E-Mail support@viromed.de

Deutsche Bank
IBAN: DE77 2007 0000 0091 3830 00
BIC: DEUTDEHHXXX
Financial Partner Distel Invest GmbH
Eugen Münch Beteiligungsgesellschaft