Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art. 28 DSGVO (Auftragsverarbeitungsvertrag)[1]

zwischen dem Auftraggeber:

(im Folgenden „Verantwortlicher“ genannt)

und

epitop GmbH

Parkring 4
85748 Garching bei München

(im Folgenden „Auftragsverarbeiter“ genannt)

[1] Kurz: AV-Vertrag

Zusammenfassung

1. Zweck der Verarbeitung

Die epitop GmbH verarbeitet personenbezogene Daten im Auftrag unserer Anwender, die im Sinne des DSGVO als „Verantwortliche“ gelten, um eine vernetzte und optimierte Datenverarbeitung für Patientenversorgung, Forschung und Prozessentwicklung zu ermöglichen. Die Verarbeitung erfolgt ausschließlich gemäß den Weisungen der Verantwortlichen.

2. Datenschutz und Sicherheit

Die epitop GmbH erfüllt die Anforderungen der DSGVO, insbesondere durch technische und organisatorische Maßnahmen zum Schutz der Daten.

Mitarbeiter sind auf das Datengeheimnis verpflichtet.

Daten werden nur in der EU/des EWR verarbeitet, es sei denn, der Verantwortliche genehmigt ausdrücklich etwas anderes.

3. Rechte und Pflichten

Unsere Anwender (die „Verantwortlichen“) bleiben Eigentümer der Daten und behalten alle Rechte.

Die epitop GmbH unterstützt den Verantwortlichen bei der Erfüllung von Betroffenenrechten (z. B. Auskunft, Berichtigung, Löschung).

Bei Vertragsende werden die Daten entweder zurückgegeben oder gelöscht, sofern keine gesetzliche Aufbewahrungspflicht besteht.

4. Vertraulichkeit und Weitergabe

Daten werden nicht an Dritte weitergegeben, außer mit Zustimmung des Verantwortlichen oder bei gesetzlicher Verpflichtung.

Unterauftragnehmer werden nur nach Information des Verantwortlichen eingesetzt und müssen die gleichen Datenschutzstandards erfüllen. Die Liste der Unterauftragnehmer finden Sie in der als Anlage3 bezeichnete Liste. Diese wird regelmäßig aktualisiert.

5. Sicherheit

Die epitop GmbH setzt Maßnahmen wie Datenverschlüsselung, Zugriffskontrollen und regelmäßige Sicherheitsprüfungen um. Backups und Notfallpläne schützen Daten vor Verlust oder Zerstörung.

6. Überwachung und Nachweise

Der Verantwortliche kann Audits durchführen, um die Einhaltung der Datenschutzvorgaben zu überprüfen. Die epitop GmbH informiert unverzüglich über Datenschutzverletzungen oder Weisungen, die gegen geltendes Recht verstoßen.

Präambel

Der Auftragsverarbeiter bietet mit seinen Lösungen dem Verantwortlichen die vernetzte Zusammenführung von Daten, sowie deren Auswertung im Rahmen der Patientenversorgung, Forschung und Prozessentwicklung an.

Hierzu werden Daten gemäß Anlage 1 aus den Einrichtungen des Verantwortlichen und ggf. gemeinsam anderen Vertragspartnern zu einer gemeinsamen Datenbasis (Patienten/Fallakte) aggregiert und mit Algorithmen verarbeitet. Der Verantwortliche hat den Auftragsverarbeiter vertraglich mit der Erbringung dieser Leistungen beauftragt.

Details finden sich in Anlage 1. Im Rahmen der Erbringung dieser Leistungen kann der Auftragsverarbeiter auch auf personenbezogene Daten zugreifen (im Folgenden „Nutzerdaten“ genannt), die durch den Verantwortlichen verarbeitet oder sonst dem Auftragsverarbeiter zur Verfügung gestellt werden, so dass es sich bei der Leistung des Auftragsverarbeiters um eine Auftragsdatenverarbeitung im Sinne des Art. 28 DSGVO handeln kann.

Zum Schutz der personenbezogenen Daten treffen die Vertragspartner die nachfolgenden Vereinbarungen zum Datenschutz.

1 Datenschutz, Auftragsdatenverarbeitung

1.1 Der Auftragsverarbeiter beachtet das jeweils geltende Datenschutzrecht und trifft geeignete organisatorische Maßnahmen, um die Einhaltung des Datenschutzrechts zu gewährleisten.

1.2 Der Auftragsverarbeiter wird nur solche Mitarbeiter einsetzen, die von ihm zuvor auf das Datengeheimnis sowie gegebenenfalls auf das Fernmeldegeheimnis nach § 88 TKG und/oder das Sozialgeheimnis nach § 35 SGB I verpflichtet worden sind. Der Auftragsverarbeiter hat die Mitarbeiter über die einschlägigen Strafvorschriften, insbesondere § 203 StGB, belehrt.

1.3 Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

2 Definitionen und Festlegungen

2.1 Gegenstand und Dauer der Aufträge ergeben sich aus der Präambel sowie aus der Laufzeit des jeweils zugrundeliegenden Hauptvertrags. Die Verarbeitung personenbezogener Daten erfolgt für die Dauer des Hauptvertrags zuzüglich etwaiger gesetzlicher Aufbewahrungsfristen. Für den Fall, dass der Verantwortliche zur Betreuung Fremdunternehmen mit der Arbeit an seinen Daten beauftragt, schließt der Verantwortliche einen eigenen Vertrag mit diesen Unternehmen ab. Der vorliegende AV-Vertrag bezieht sich ausschließlich auf Leistungen des Auftragsverarbeiters.

2.2 Soweit der Auftragsverarbeiter Zugriff auf personenbezogene Daten hat, die der Verantwortliche verarbeitet oder dem Auftragsverarbeiter sonst zur Verfügung stellt und die der Auftragsverarbeiter zur Erbringung der von ihm geschuldeten Leistungen verarbeitet, erfolgt dies im Auftrag und auf Weisung des Verantwortlichen gem. Art. 28 DSGVO.

2.3 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.4 Die Nutzerdaten sind in Anlage 1 näher spezifiziert.

3 Weisungsgebundenheit; Erhebung, Nutzung und Verarbeitung der Daten durch den Auftragsverarbeiter

3.1 Der Auftragsverarbeiter wird die Nutzerdaten nur im Rahmen der dokumentierten Weisungen des Verantwortlichen verarbeiten. Mündliche Weisungen wird der Verantwortliche unverzüglich schriftlich bestätigen, eine E-Mail ist ausreichend. Der Auftragsverarbeiter wird die Nutzerdaten nur in dem Umfang verarbeiten, wie dies zur Erfüllung der von dem Auftragsverarbeiter vertraglich geschuldeten Leistungen erforderlich ist. Der Auftragsverarbeiter wird geeignete technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die einschlägigen Vorschriften der DSGVO zu erfüllen, insb. die in Art. 32 DSGVO genannten Anforderungen.

3.2 Die konkreten Maßnahmen ergeben sich aus dem Dokument „Technische und Organisatorische Maßnahmen“, welches diesem AV-Vertrag als Anlage 2 beigefügt ist.

4 Pflichten des Auftragsverarbeiters, Rechte des Verantwortlichen

4.1 Der Auftragsverarbeiter wird den Verantwortlichen auf sein schriftliches Verlangen bei der Wahrung der Rechte der betroffenen Personen, insb. im Hinblick auf die Benachrichtigung, Auskunftserteilung sowie die Berichtigung, Sperrung oder Löschung der Nutzerdaten im Rahmen seiner Möglichkeiten unterstützen, insbesondere wird der Auftragsverarbeiter

4.2 angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Pflicht des Verantwortlichen zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen, wenn der Verantwortliche dem Auftragsverarbeiter diese Anträge übermittelt und unter Zitat des entsprechenden Gesetzestexts nachweist, dass diese Anträge berechtigt sind.

4.3 Erhält der Auftragsverarbeiter eine Anfrage einer betroffenen Person im Zusammenhang mit der Verarbeitung personenbezogener Daten aus diesem Auftragsverhältnis, wird er - den Verantwortlichen hierüber unverzüglich, spätestens innerhalb von drei (3) Werktagen, informieren. Der Auftragsverarbeiter wird solche Anfragen nicht eigenständig beantworten, sondern ausschließlich nach Weisung des Verantwortlichen tätig werden.

4.4 Darüber hinaus unterstützt der Auftragsverarbeiter den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten unterstützen (Sicherheit der Verarbeitung; ggf. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde; ggf. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; bei voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen Datenschutz-Folgenabschätzung mit ggf. vorheriger Konsultation der Datenschutzbehörde), soweit der Verantwortliche gegenüber dem Auftragsverarbeiter nachweist, dass der Verantwortliche im konkreten Einzelfall, für den dieser Unterstützung verlangt, derartige Pflichten hat.

4.5 Der Auftragsverarbeiter wird alle Nutzerdaten vertraulich behandeln und sicher verwahren. Der Auftragsverarbeiter darf die Nutzerdaten nicht an Dritte weitergeben, es sei denn, der Verantwortliche hat zuvor ausdrücklich zugestimmt oder der Auftragsverarbeiter einer gesetzlichen Pflicht nachkommen muss.

4.6 Der Auftragsverarbeiter ist berechtigt, für die Datenverarbeitung gemäß diesem AV-Vertrag Unterauftragnehmer einzusetzen. Der Auftragsverarbeiter wird den Verantwortlichen mindestens vierzehn (14) Kalendertage vor der Hinzuziehung neuer oder dem Austausch bestehender Unterauftragsverarbeiter informieren. Der Verantwortliche hat das Recht, aus wichtigem Grund, insbesondere aus datenschutzrechtlichen Gründen, gegen die beabsichtigte Änderung Einspruch zu erheben.

4.7 Im Falle eines berechtigten Einspruchs wird der Auftragsverarbeiter die geplante Änderung nicht umsetzen oder gemeinsam mit dem Verantwortlichen eine alternative Lösung abstimmen.

4.8 Soweit der Verantwortliche von dieser Möglichkeit Gebrauch macht, hat der Auftragsverarbeiter sicherzustellen, dass alle in diesem AV-Vertrag und in Art. 28 DSGVO genannten Pflichten des Auftragsverarbeiters auch von den betreffenden Unterauftragsverarbeitern eingehalten werden, 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.

4.9 Der Verantwortliche hat das Recht, im Einvernehmen mit dem Auftragsverarbeiter Audits durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig, jedoch mindestens vier (4) Wochen vorher anzumelden sind, von der Einhaltung dieses AV-Vertrages durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Für die Ermöglichung von Kontrollen durch den Verantwortlichen kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

4.10 Der Auftragsverarbeiter wird dem Verantwortlichen auf seine Anforderung geeignete Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO beschriebenen Pflichten zur Verfügung stellen, wenn der Verantwortliche konkret unter Zitat der entsprechenden gesetzlichen Formulierung benennt, für welche Pflicht er von dem Auftragsverarbeiter gem. Art 28 DSGVO Informationen benötigt.

4.11 Wenn der Auftragsverarbeiter erfährt, dass im seinem Verantwortungsbereich gegen geltendes Datenschutzrecht oder gegen Regelungen aus diesem AV-Vertrag verstoßen worden ist, wird der Auftragsverarbeiter den Verantwortlichen unverzüglich darauf hinweisen.

4.12 Der Verantwortliche darf dem Auftragsverarbeiter Weisungen nur im Rahmen der vertraglichen Pflichten des Auftragsverarbeiters erteilen.

5 Hinweispflicht, Pflichten bei Vertragsbeendigung

5.1 Der Auftragsverarbeiter wird unverzüglich den Verantwortlichen darauf hinweisen, wenn der Auftragsverarbeiter der Ansicht ist, dass eine Weisung von dem Verantwortlichen gegen geltendes Datenschutzrecht verstößt.

5.2 Spätestens drei (3) Monate nach Beendigung des AV-Vertrags wird der Auftragsverarbeiter die von dem Verantwortlichen übergebenen Datenträger, die Nutzerdaten enthalten, an den Verantwortlichen zurückgeben und die bei dem Auftragsverarbeiter gespeicherten Nutzerdaten nach Wahl von dem Verantwortlichen entweder löschen oder zurückgeben. Dies gilt nicht, soweit der Auftragsverarbeiter aufgrund Unionsrecht oder dem Recht der Mitgliedstaaten der EU zur Aufbewahrung der personenbezogenen Daten verpflichtet ist. Im Falle einer solchen längeren gesetzlichen Aufbewahrungspflicht wird der Auftragsverarbeiter die betreffenden Datenträger zurückgeben und die Nutzerdaten löschen, sobald das Gesetz dies zulässt.

6 Schlussbestimmungen

6.1 Dieser AV-Vertrag ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Das Gleiche gilt für Änderungen.

6.2 Sollten Bestimmungen dieses AV-Vertrages rechtsunwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die rechtsunwirksamen Bestimmungen sind von den Vertragspartnern unverzüglich durch solche Bestimmungen zu ersetzen, die dem wirtschaftlich gewollten Zweck der Vertragspartner entsprechen. Das gilt entsprechend für Lücken.

6.3 Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftragsverarbeiters.

Anlage 1 Nutzerdaten

Der Auftragsverarbeiter verarbeitet nachfolgend genannten Nutzerdaten:

Kategorien betroffener Personen:

- Patienten des Verantwortlichen
- Mitarbeiter des Verantwortlichen
- Dienstleister des Verantwortlichen

Art der personenbezogenen Daten:

- Allgemeine Personendaten (Name, Geburtsdaten, Anschrift, Telefonnummer, Familienstand, Staatsangehörigkeit, E-Mail-Adresse, Krankenkassen; Beruf, Arbeitgeber, Beschäftigungsverhältnis, Ethnische Zugehörigkeit
- Kennnummern (Kundennummer, Nummer bei den Krankenkassen, sonst. Versicherungsnummer., Arztnummer)
- Bankdaten
- Administrative Daten (Betriebsstättenbezogene Daten)
- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur)
- Medizinische Dokumentationsdaten
- Onlinedaten (IP-Adresse)
- Software-Lizenzdaten, Versionsdaten
- Hard- und Softwareinformationen

Zwecke der Verarbeitung

- Dokumentation der Betreuung und Versorgung von Patienten und Kunden inklusive Maßnahmen, Verordnungen und damit verbundene Aktionen von Patienten und Kunden
- Rechtssichere Identifikation von Patienten und/oder Kunden sowie die Verhinderung von Daten- und Identitätsmissbrauch.
- Archivierung von Daten
- Bereitstellung von ausgewählten Daten für berechtigte Beteiligte im Versorgungs- und Betreuungsprozess
- Unterstützung von Studien und Evaluationen zur Verbesserung von Therapien, Versorgung und Betreuung von Kunden und Patienten und damit verbundene Entwicklungen von Produkten und Lösungen
- Entwicklung und Betreuung von Versorgungspfaden
- Fachliche, medizinische und organisatorische Verbesserung der Gesundheits- und Patientenversorgung

- KI-gestützte Analyse und Strukturierung medizinischer Daten zur Unterstützung der Patientenversorgung und medizinischen Dokumentation
- Erstellung und Speicherung strukturierter Analyseergebnisse als Bestandteil der Patienten- bzw. Fallakte
- Bereitstellung von Analyseartefakten zur Unterstützung lokaler Assistenz- und Auswertungssysteme

Art der Verarbeitung / Services

- Verwaltung, Archivierung, Auswertung und gesicherte Weitergabe von Daten an berechtigte Dritte im Rahmen der Patientenversorgung oder Kundenbetreuung.
- Bereitstellung und Weiterleitung von relevanten Daten an berechtigte Dritte im Rahmen einer gemeinsamen Versorgung und Betreuung
- Auswertung der verarbeiteten Daten im Rahmen der Betreuung und Versorgung
- Auswertung von Daten zur Entwicklung und Verbesserung von Lösungen, die die Betreuung und Versorgung von Kunden und Patienten verbessern
- Auswertung von Daten zu Betreuung, Versorgung, Abrechnung und Forschungszwecken
- Zusammenführung und Konsolidierung von Daten
- Übermittlung ausgewählter Daten an berechtigte technische Dienstleister zur KI-gestützten Analyse im Rahmen der beauftragten Verarbeitung
- Rückübernahme und Speicherung der erzeugten Analyseergebnisse als Bestandteil der Patienten- bzw. Fallakte
- Verarbeitung strukturierter KI-generierter Analyseinformationen zur Unterstützung weiterer Auswertungs- und Assistenzfunktionen

Anlage 2

Technische und organisatorische Maßnahmen

Allgemeine Maßnahmen

- Vorhandensein von internem IT-Sicherheitskonzept und IT-Sicherheitsrichtlinien.
- Datenverarbeitung ist in Arbeits- und Prozessbeschreibungen schriftlich geregelt.
- Fremdfirmen haben keinen Zugriff auf Datenverarbeitung.
- Schriftliche Bestellung eines Datenschutzbeauftragten. Datenschutzbeauftragter der epitop GmbH ist erreichbar unter: E-Mail: datenschutz@epitop.com
- Verpflichtung aller Mitarbeiter nachweislich auf das Datengeheimnis sowie ggf. § 88 TKG und ggf. § 35 SGB I, Belehrung über den § 203 StGB.
- Regelmäßige Kontrolle bzgl. Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen.
- Vorhandensein von Verzeichnissen von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO, soweit eine Verpflichtung gem. Art. 30 Abs. 5 DSGVO besteht.
- Namentliche Nennung der Ansprechpartner (IT/DV-Verantwortlicher und Daten-schutzbeauftragter) zur Klärung fachlicher, technischer und organisatorischer Fragen.
- Pseudonymisierung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.
- Verschlüsselung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.

Zugangskontrolle

Die Zugangskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt (physikalische Sicherheit) zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen im Einzelnen:

- Aufgrund der Lage der Geschäftsräume sind Einwirkversuche von außen über die Fenster ausreichend verhindert. Die Geschäftsräume sind nur durch Personal mit entsprechenden Transpondern oder Schlüsseln zu betreten.
- zusätzlich werden außerhalb der Bürozeiten einbruch- und feuerhemmende Sicherheitstüren verschlossen.
- Ausgabe und Rückgabe von Transpondern und Schlüsseln ist geregelt, mit Schlüsselbuch bzw. durch Systemdokumentation.
- Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern von epitop im Büro begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten.

- epitop verpflichtet auch Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren.
- Der Zutritt zu den Serverräumen ist durch eine separate digitale Schließanlage abgesichert. Die Zutrittserlaubnis ist auf das unbedingt notwendige Personal (Systemadministratoren) beschränkt. Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind, er- halten keinen Zutritt zu den Serverräumen.

Datenträgerkontrolle

Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.

Maßnahmen im Einzelnen:

- Externer Zugriff von epitop-Mitarbeitern auf epitop-Server ist nur via VPN und Authentifizierung am epitop-LAN möglich.
- Trennung Gast-WLAN vom Firmennetzwerk.
- epitop-WLAN wird mit WPA2 betrieben.
- Anti-Viren-Software auf allen eingesetzten IT/DV-Anlagen.
- Akten unter Verschluss. Zugang nur für berechtigte Personen.
- Der Zugang zu den IT-Systemen ist durch Zugangsberechtigungen geregelt. Eine Firewall verhindert ungewollte Zugriffe von außen.
- Werden Passwörter mehrfach fehlerhaft eingegeben, erfolgt eine Sperrung. Diese kann nur durch einen Administrator rückgängig gemacht werden.
- Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten wie möglich aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server von epitop).
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an die epitop zurück.

Speicherkontrolle

Die Speicherkontrolle umfasst Maßnahmen, mit denen die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.

Maßnahmen im Einzelnen:

- Zugriffe auf die Server von epitop erfolgen durch Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen. Bei Daten von Auftraggebern wird die Zugriffsberechtigung in der Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art: 28 DSGVO (Auftragsdatenverarbeitung) geregelt.
- Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter nur auf die Datenbanken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen.
- Bei Zugriff auf Daten beim Auftraggeber ist durch die von epitop eingesetzten Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter von epitop ausschließlich

auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass alle Zugriffe in der Kundendokumentation protokolliert werden.

- Wenn ein Mitarbeiter ausscheidet, werden ihm die Zugriffsrechte entzogen.
- Die Datenfernübertragungssysteme von epitop sind mit Datenverschlüsselung versehen und werden auf dem jeweils aktuellen technischen Stand gehalten.
- Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Auftraggeberbereich zu lesen, zu kopieren, zu ändern oder zu entfernen.
- Wenn epitop die Daten aus dem Auftraggeberbereich nicht mehr benötigt, werden die Datenträger nach DIN 32757-1 und gemäß den Bestimmungen des Datenschutzes vernichtet. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht.
- Siehe im Übrigen Datenträgerkontrolle und Zugriffskontrolle.

Benutzerkontrolle

Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.

Maßnahmen im Einzelnen:

Siehe im Übrigen Datenträgerkontrolle und Zugriffskontrolle.

Zugriffskontrolle

Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Maßnahmen im Einzelnen:

- Vorhandensein eines Berechtigungskonzepts.
- Datenträgerverwaltung, Datensicherung, Aufbewahrung außerhalb des Gebäudes, Verschlüsselung.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.
- Zugriff auf Notebooks, PC und Server von epitop nur mit Username und Passwort möglich.
- Passwörter unterliegen definierten Passwortrichtlinien nach dem Stand der Technik (mindestens 12 Zeichen, Komplexitätsanforderungen, regelmäßige Überprüfung). Arbeitsplatzrechner, Notebooks und Server sind durch individuelle Benutzerkonten, automatische Bildschirmsperren sowie durch eine Verschlüsselung der Datenträger abgesichert.
- Administratoren sind für Vergabe und regelmäßige Änderung von Passwörtern verantwortlich.
- Betrieb von Arbeitsplatz-PC und Servern nur nach Anmeldung mit Benutzername und Passwort.
- Automatische Bildschirmsperre mit Passwort-Aktivierung.
- Zugangsprotokollierung.

- Sperrung nach mehrmaligen fehlerhaften Anmeldeversuchen.
- Löschung und Zwischenlagerung defekter Datenträger bis zur datenschutzkonformen Vernichtung.
- Vernichtung ausgedruckter Daten im Aktenvernichter bzw. durch zugelassene Fachunternehmen.
- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDAs, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung schriftlich geregelt.

Übertragungskontrolle

Die Übertragungskontrolle umfasst Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Maßnahmen von epitop im Einzelnen:

- Regelungen zur Datenübertragung sind vorhanden.
- Übermittlung und Zur-Verfügung-Stellen von Daten wird protokolliert.
- Die epitop bearbeitet die Daten nur im Rahmen der Weisungen des Auftraggebers.

Eingabekontrolle

Die Eingabekontrolle umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt worden sind.

Maßnahmen von epitop im Einzelnen:

- Regelungen zur Dateneingabe sind vorhanden.
- Erstellung und Änderung von Daten wird protokolliert.
- Werden personenbezogene Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche an epitop übertragen, werden diese Daten nach Beendigung der Fehlersuche gelöscht. Eine Veränderung oder Entfernung im Sinne des Datenschutzrechts findet nicht statt, es sei denn, dass der Auftraggeber dies vorher ausdrücklich schriftlich beauftragt hat.

Transportkontrolle

Die Transportkontrolle umfasst 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.

Maßnahmen im Einzelnen:

- Firewall.
- Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung.
- Statistiken mit personenbezogenen Inhalten werden nur im Auftrag von Auftraggeber und

nur an berechtigte Personen bei Auftraggeber übermittelt.

Wiederherstellbarkeit

Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Maßnahmen im Einzelnen:

- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Datenträgerverwaltung, Datensicherung, Aufbewahrung außerhalb des Gebäudes.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.

Zuverlässigkeit

Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Maßnahmen im Einzelnen:

Siehe Verfügbarkeitskontrolle.

Datenintegrität

Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Maßnahmen im Einzelnen:

Siehe Verfügbarkeitskontrolle.

Auftragskontrolle

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.

Maßnahmen im Einzelnen:

- Alle epitop-Mitarbeiter sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Alle vom Auftraggeber bereit gestellten Daten verbleiben ausschließlich in der Verfügungsmacht von epitop.
- Weitergabe personenbezogener Daten erfolgt nur nach Einwilligung vom Auftraggeber.
- Dienstleister von epitop unterliegen Überprüfungen (Lieferantenaudits).
- Alle Mitarbeiter von epitop, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen im Einzelnen:

- Tägliche Datensicherung.
- Feuerlöscher in ausreichender Anzahl im Gebäude.
- Brandschutztüren.
- Vorgaben des Brandschutzes werden eingehalten und regelmäßig durch externe Prüfungen verifiziert.
- Rauchverbot im Serverraum.
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz.
- Back-Up-Verfahren für Server und Arbeitsplatz-PCs.
- Alle betroffenen Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.
- Von einem Auftraggeber übergebene Datenträger werden unter Verschluss verwahrt.
- Sicherungskopien außerhalb des Gebäudes.
- Gespiegelte Server-Festplatten.
- Virenschutzprogramme auf allen Computersystemen.
- Intrusion Detection System.
- epitop setzt eine Firewall und aktuelle Virenscanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers ein. Die Virensignaturen des verwendeten Virenscanners werden täglich mehrmals aktualisiert.
- Arbeitsplatzrechner werden laufend durch aktuelle Scannerprogramme auf schadhafte Software überprüft. E-Mail-Anhänge werden auf Infizierung überwacht.
- Die Mitarbeiter sind angehalten, personenbezogene Daten, die sie auf ihren Notebooks gespeichert haben, möglichst bald auf ein zentrales System von epitop zu überspielen.
- Schriftlicher Notfallplan.

Trennbarkeit

Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen im Einzelnen:

Wenn Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche oder deren Wiederherstellung übertragen werden, werden diese gesondert von Daten anderer Auftraggeber gespeichert.

Anlage 3

3.1 Allgemeine Unterauftragnehmer

Diese Unterauftragnehmer können im Rahmen des standardmäßigen und Reibungslosen Betriebs der epitop Lösungen herangezogen werden

Unterauftragnehmer	Auftragszweck
centron GmbH Heganger 29, D-96103 Hallstadt	Rechenzentrum für den Betrieb einzelner zentraler Komponenten der Lösungen
Ionos SE Elgendorfer Str. 57, 56410 Montabaur	Rechenzentrum für den Betrieb einzelner zentraler Komponenten der Lösungen
Strato AG, Otto-Ostrowski-Straße 7, 10249 Berlin	Rechenzentrum für den Betrieb einzelner zentraler Komponenten der Lösungen
InterNetX GmbH, Johanna-Dachs-Str. 55, 93055 Regensburg	Rechenzentrum für den Betrieb einzelner zentraler Komponenten der Lösungen
Zoho Corporation GmbH Trinkausstr. 7, 40213 Düsseldorf	Kunden- und Ticketverwaltung
TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen	Fernwartungstool zur Kommunikation zwischen Auftraggeber und Auftragnehmer
Masterplan Tech Solutions GmbH Jacob-Klar-Str. 4 80802 München	KI-gestützte Analyse und Strukturierung medizinischer Daten zur Erstellung von KI-generierter Analyseinformationen (Artefakte) im Rahmen der Patientenversorgung.
MPiriQ Science Technologies GmbH Pennstraße 62 81549 München	KI-gestützte Analyse und Strukturierung medizinischer Daten zur Erstellung von KI-generierter Analyseinformationen (Artefakte) im Rahmen der Patientenversorgung.

3.2. Optionale Unterauftragnehmer

Sofern einzelne Vorhaben und Aufträge die Integration weiterer Unterauftragnehmer, über die oben genannten hinaus, bedürfen, werden diese nach gesonderter Vereinbarung und Auftragsbestätigung inkl. Bezeichnung des Unterauftragnehmers und Auftragszweck benannt und werden somit Teil dieser Vereinbarung.