Kulzer Auftragsdatenverarbeitungsbedingungen 06/2018

§ 1 Definitionen

Im Rahmen der Auftragsdatenverarbeitung werden die folgenden Begriffe verwendet:

„Auftraggeber“ ist jede Person, die Kulzer mit der Verarbeitung Personenbezogener Daten beauftragt.

“Betroffene Person” ist eine natürliche Person, auf die sich die personenbezogenen Daten beziehen und die hierdurch identifiziert werden kann oder identifizierbar wird. Dies ist der Fall, sofern eine Zuordnung der Person zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen personenbezogenen Merkmalen dieser Person sind, erfolgt. Die im Rahmen des MSA betroffenen Personen sind in Anhang 1 erfasst.

“Datenschutzvorschriften” bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), zusammen mit jeglichen sonstigen Gesetzen auf der Grundlage dieser Richtlinie oder Verordnung, sämtliche sonstigen geltenden, anwendbaren Gesetze jedes sonstigen Landes hinsichtlich des Schutzes der personenbezogenen Daten oder Datenschutz, in ihrer zum jeweiligen Zeitpunkt geänderten oder ersetzten Fassung;

„MSA“ ist eine oder mehrere Vereinbarungen über die Erbringung für den Auftraggeber gewisser Dienstleistungen in Zusammenhang mit der Herstellung von Zahnersatz und damit in Zusammenhang stehende Serviceleistungen durch Kulzer für den Auftraggeber.

„Parteien“ sind die Vertragsparteien des MSA.

“Personenbezogene Daten” sind solche Daten, die zur Identifikation einer natürlichen Person genutzt werden können. Die jeweiligen Kategorien von Personenbezogenen Daten sind in Anhang 1 festgelegt.

“Standardvertragsklauseln” bezeichnet die Standardvertragsklauseln, zu denen die Europäische Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG befunden hat, dass diese ausreichende Garantien für die Übermittlung Personenbezogener Daten an ein Drittland bieten, oder die von der Europäischen Kommission oder einer Aufsichtsbehörde festgelegten Datenschutzklauseln, die von der Europäischen Kommission gemäß dem in Artikel 93 Absatz 2 der Verordnung (EU) Nr. 2016/679 genannten Verfahren gebilligt wurden. Gemäß der Datenschutz-Grundverordnung festgelegte Datenschutzklauseln ersetzen und gehen etwaigen gemäß Richtlinie 95/46/EG festgelegten Standardvertragsklauseln vor, soweit sie dieselbe Art von Datenübermittlungsbeziehung abdecken sollen.

“Unterauftragsdatenverarbeiter” ist jeder Subunternehmer, der von Kulzer beauftragt wurde, die Verarbeitung der Personenbezogenen Daten ganz oder teilweise durchzuführen.

„Verantwortlicher“ ist die Person im Sinne des Art. 4 Nr. 7 DS-GVO

“Verarbeitungsvorgang” oder “verarbeitet” bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

§ 2 Gegenstand, Dauer und Art sowie Zweck der Auftragsdatenverarbeitung

Diese Auftragsdatenverarbeitungsvereinbarung samt Anlagen (nachstehend „**ADV**“), insbesondere die Bestimmungen für den Umgang mit den Personenbezogenen Daten und die technisch organisatorischen Maßnahmen sind für die Handhabung der Personenbezogenen Daten der Betroffenen Personen während der Dauer und in Abwicklung des MSA maßgebend.

Im Rahmen des MSA übernimmt Kulzer für den Auftraggeber u.a. die Bereitstellung von Lösungen zur Erstellung von Dentalprothetik sowie die Umsetzung der gefundenen Lösung. Weiterhin erbringt der Kulzer Supportleistungen für den Auftraggeber. In diesem Zusammenhang besteht die Möglichkeit, dass Kulzer mit im **Anhang 1** aufgeführten Personenbezogenen Daten in Berührung kommt und diese verarbeitet.

Die Bearbeitung von Personenbezogenen Daten durch Kulzer erfolgt nur nach vorheriger schriftlicher Auftragserteilung und nur im vertraglich festgelegten Umfang und für den vereinbarten Zweck und nach den Weisungen des Auftraggebers.

Die durch Kulzer verarbeiteten Personenbezogenen Daten dienen ausschließlich den folgenden Zwecken:

- Vertragsdurchführung, inkl. Servicedienstleistungen
- Forschung & Entwicklung
- Statistische Zwecke

Eine anderweitige Nutzung der Personenbezogenen Daten für eigene oder fremde Zwecke erfolgt nicht. Kulzer beachtet dabei jederzeit die einschlägigen datenschutzrechtlichen Bestimmungen. Kulzer verpflichtet sich insbesondere bei der Erbringung der Leistungen die Grundsätze der Datensparsamkeit und Datenvermeidung zu beachten.

§ 3 Anwendungsbereich und Verantwortlichkeit

Kulzer verarbeitet Personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im MSA und in der dortigen Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser ADV für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an Kulzer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich gegenüber dem Verantwortlichen und Kulzer.

Die Weisungen werden anfänglich durch den MSA festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von Kulzer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im MSA nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 4 Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie die Wahrung der Rechte der Betroffenen Personen ist der Auftraggeber verantwortlich. Das alleinige Verfügungsrecht über die Personenbezogenen Daten verbleibt bei dem Auftraggeber. Insbesondere ist der Auftraggeber für die Datenweitergabe an Kulzer sowie für die Wahrung der Rechte der Betroffenen Personen verantwortlich. Darüber hinaus verpflichtet sich der Auftraggeber zur Einhaltung sämtlicher einschlägiger datenschutzrechtlicher Vorschriften im Rahmen der Durchführung des MSA. Der Auftraggeber ist für die Vollständigkeit und Richtigkeit der zu verarbeitenden Daten verantwortlich und sichert zu, dass die Daten im Hinblick auf den Verwendungszweck korrekt und vollständig sind.

Der Auftraggeber ist verpflichtet und berechtigt, vor Beginn der Datenverarbeitung und sodann in regelmäßigen Abständen die Einhaltung der von Kulzer getroffenen technischen und organisatorischen Maßnahmen nach **Anlage 2** zu prüfen und schriftlich zu bestätigen. Einzelheiten ergeben sich aus § 9 dieser ADV.

Sofern der Auftraggeber Fehler oder Unregelmäßigkeiten bei der vorbenannten Prüfung feststellt, wird er Kulzer hierüber unverzüglich informieren.

Im Hinblick auf den Schutz der Rechte der Betroffenen Personen gemäß den geltenden Datenschutzvorschriften ermöglicht der Auftraggeber die Ausübung der Rechte der Betroffenen Personen und stellt sicher, dass den Betroffenen Personen eindeutige, transparente, verständliche und leicht zugängliche Informationen in klarer Sprache über die hier dargestellte Verarbeitung zur Verfügung gestellt werden.

Der Auftraggeber ist verpflichtet, alle im Rahmen des MSA und der ADV erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen von Kulzer vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarungen bestehen.

§ 5 Technische und organisatorische Maßnahmen nach § 32 DSGVO

Kulzer hat geeignete technische und organisatorische Maßnahmen zum Schutz der Personenbezogenen Daten vor unbeabsichtigtem, unbefugtem oder gesetzwidrigem Zugriff, Offenlegung, Änderung, Verlust oder Zerstörung umgesetzt und wird diese beibehalten. Diese Maßnahmen umfassen u.a.:

- Verhinderung des Zugriffs auf Systeme zur Verarbeitung Personenbezogener Daten durch unbefugte Personen (physische Zugriffskontrolle)
- Verhinderung der Nutzung von Systemen zur Verarbeitung Personenbezogener Daten ohne entsprechende Autorisierung (logische Zugriffskontrolle)
- Gewährleistung, dass zur Nutzung eines Systems zur Verarbeitung Personenbezogener Daten berechtigte Personen nur auf Personenbezogene Daten zugreifen können, auf die sie gemäß ihren Zugriffsrechten zugreifen dürfen, und dass die Personenbezogenen Daten im Zuge der Verarbeitung ohne entsprechende Autorisierung nicht gelesen, kopiert, verändert oder gelöscht werden können (Datenzugriffskontrolle)
- Gewährleistung, dass Personenbezogene Daten während der elektronischen Übermittlung, des Transports oder der Speicherung auf Speichermedien ohne Autorisierung nicht gelesen, kopiert, geändert oder gelöscht werden können und dass die Zieleinrichtungen für jede Art von Übertragung Personenbezogener Daten mittels Datenübertragungseinrichtungen festgelegt und überprüft werden können (Datenübertragungskontrolle)
- Gewährleistung der Einrichtung eines Prüfpfads, um zu dokumentieren, ob und von wem Personenbezogene Daten in Systeme zur Verarbeitung Personenbezogener Daten eingegeben, darin verändert oder daraus entfernt wurden (Eingabekontrolle)
- Gewährleistung, dass verarbeitete Personenbezogene Daten einzig und allein gemäß den Weisungen verarbeitet werden (Weisungskontrolle)
- Gewährleistung, dass Personenbezogene Daten vor unbeabsichtigter Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

Die technischen und organisatorischen Maßnahmen sind in **Anhang 2** zu dieser ADV beschrieben. Kulzer hat das Recht, diese Maßnahmen systematisch an die Entwicklung der Verordnungen, der Technik und anderer Aspekte anzupassen und stellt sicher, dass sie gegebenenfalls durch geeignete technische und organisatorische Maßnahmen von Unterauftragsdatenverarbeitern ergänzt werden. In jedem Fall müssen die umgesetzten technischen und organisatorischen Maßnahmen ein Schutzniveau gewährleisten, das den Risiken angemessen ist, die von der Datenverarbeitung und der Art der zu schützenden Personenbezogenen Daten ausgehen; dabei müssen außerdem der Stand der Technik und die Kosten ihrer Umsetzung berücksichtigt werden.

Innerhalb der Laufzeit des MSA und dieser ADV kann der Auftraggeber von Kulzer verlangen, innerhalb einer angemessenen Zeitspanne eine aktuelle Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen zu übermitteln.

§ 6 Ort der Verarbeitung

Vorbehaltlich § 7 dieser ADV können Personenbezogene Daten, die Kulzer im Auftrag des Auftraggebers verarbeitet, in jedem Land verarbeitet werden, in dem Kulzer, seine verbundenen Unternehmen und befugten Unterauftragsdatenverarbeiter Einrichtungen zur Erbringung der Dienstleistungen unterhalten. Der Auftraggeber erteilt Kulzer die Befugnis, im Zusammenhang mit der Erbringung der Dienstleistungen Personenbezogene Daten in jedes dieser Länder zu übermitteln und in jedem dieser Länder zu verarbeiten. Jede Übermittlung von einem Rechtsraum in einen anderen Rechtsraum (zum Zwecke dieses Artikels stellt die EU einen einzigen Rechtsraum dar) erfolgt nur unter Einhaltung der geltenden Datenschutzvorschriften, wie beispielsweise der Ausfertigung eines den Standardvertragsklauseln unterliegenden zusätzlichen Datenverarbeitungsvertrags (je nach Sachverhalt).

Kulzer wird das geografische Gebiet, von dem aus der Auftraggeber oder die Kunden des Auftraggebers Personenbezogene Daten verarbeiten können, weder kontrollieren noch einschränken.

§ 7 Unterauftragsdatenverarbeiter

Der Auftraggeber erkennt an und ist ausdrücklich damit einverstanden, dass Kulzer Personenbezogene Daten an dritte Unterauftragsdatenverarbeiter zur Erbringung der Dienstleistungen übermitteln darf, sofern diese Übermittlung gemäß den Bedingungen dieses Paragrafen erfolgt.

Zwischen diesen Unterauftragdatensverarbeitern und Kulzer bestehen schriftliche Verträge, die Verpflichtungen enthalten, deren Schutzniveau nicht niedriger ist als in dieser ADV einschließlich der Verpflichtungen gemäß den Standardvertragsklauseln, soweit anwendbar. Der Auftraggeber ermächtigt Kulzer ausdrücklich, die Standardvertragsklauseln in seinem Auftrag gegenüber den entsprechenden Unterauftragsdatenverarbeitern auszufertigen und durchzusetzen, wobei diese Standardvertragsklauseln durch die vorliegende ADV geregelt werden.

Kulzer informiert den Auftraggeber mit dieser ADV über alle Kategorien der Unterauftragsdatenverarbeiter, die Personenbezogene Daten in Verbindung mit dem MSA verarbeiten, vgl. Anhang 1. Der Auftraggeber wird im Rahmen der Anbahnung des jeweiligen Einzelauftrags über den konkreten Unterauftragsdatenverarbeiter informiert und erklärt vor, spätestens jedoch mit der jeweiligen Erteilung eines Einzelauftrags im Rahmen des MSA seine Zustimmung zur Inanspruchnahme des jeweiligen Unterauftragsdatenverarbeiter durch Kulzer.

Kulzer ist gegenüber den Unterauftragsdatenverarbeitern berechtigt und verpflichtet, die Umsetzung des Datenschutzes und insbesondere die getroffenen technischen und organisatorischen Maßnahmen des Unterauftragsnehmers im erforderlichen Umfang zu kontrollieren.

§ 8 Berichtigung, Einschränkung und Löschung von Daten

Die Löschung oder Einschränkung der Verarbeitung erfolgt nach schriftlicher Weisung des Auftraggebers und vorbehaltlich etwaiger gesetzlicher Weigerungsgründe Kulzers. Kulzer behält sich vor, Daten eigenmächtig zu löschen oder deren Verarbeitung einzuschränken soweit diese für die Durchführung des MSA nicht mehr erforderlich sind oder eine Einwilligung nicht weiter wirksam ist.

Sofern eine Betroffene Person von Kulzer die Löschung, Berichtigung oder Auskunft seiner Daten verlangt, wird Kulzer diese Betroffene Person an den Auftraggeber verweisen, sofern eine solche Zuordnung mit den vorliegenden Daten möglich ist. Weiterhin wird der Kulzer den Auftraggeber auf Weisung im Rahmen seiner Möglichkeiten bei der Umsetzung der Forderung unterstützen.

§ 9 Kontroll- und Auditrechte des Verantwortlichen

Für die Beurteilung der Zulässigkeit der Verarbeitung der Personenbezogenen Daten sowie für die Ausführung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und steht insoweit auch für den Verantwortlichen ein. Der Kulzer stellt auf Anfrage die nach Artikel 28 DSGVO notwendigen Informationen dem Auftraggeber oder dem Verantwortlichen zur Verfügung.

Der Auftraggeber und der Verantwortliche sind unter Einschaltung eines unabhängigen datenschutzrechtlichen Prüfinstituts (TÜV, Dekra o.a.) („Prüfer“) ausschließlich auf deren Kosten befugt, vor und nach Beginn der Datenverarbeitung während der üblichen Geschäftszeiten im erforderlichen Umfang und mit vorheriger Ankündigung die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere der von Kulzer getroffenen technischen und organisatorischen Maßnahmen, zu kontrollieren. Jegliche Informationen von Kulzer, mit Ausnahme der Persönlichen Daten der Betroffenen Person, sind vertrauliche Informationen und dürfen nur dem Prüfer zugänglich gemacht werden. Der Verantwortliche bzw. Auftraggeber und jeweilige Prüfer sind befugt, schriftliche Auskünfte und die Vorlage von Nachweisen über die eingerichteten Datenschutzmaßnahmen sowie über die Art und Weise ihrer technischen und organisatorischen Umsetzung zu verlangen. Darüber hinaus ist der Prüfer befugt, das Grundstück und die Betriebsstätten von Kulzer zu betreten, nach seinem Ermessen Prüfungen und Besichtigungen vorzunehmen und im erforderlichen Umfang in verarbeitungsrelevante Unterlagen, Verarbeitungs- und Ablaufprotokolle, Systeme und gespeicherte Daten und in Regelungen, Richtlinien und Handbücher zur Regelung der beauftragten Datenverarbeitung einzusehen. Dazu gehören auch Nachweise hinsichtlich der Bestellung eines Datenschutzbeauftragten, die Verpflichtung der Mitarbeiter auf die Wahrung der Vertraulichkeit und technische und organisatorische Konzepte, z. B. einschlägige Verfahrensanweisungen und auch Verträge mit Unterauftragsdatenverarbeitern.

Die vorgenannten Rechte des Auftraggebers oder Verantwortlichen bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus dem MSA, mindestens jedoch solange Kulzer Personenbezogene Daten aus den beauftragten Verarbeitungen speichert.

In besonderen Fällen, insbesondere, wenn Verarbeitungsprobleme bestehen, meldepflichtige Vorfälle aufgetreten sind oder aufsichtsrechtliche Maßnahmen anstehen oder eingeleitet worden sind, kann die Prüfung durch den Prüfer auch ohne vorherige Anmeldung erfolgen.

§ 10 Verhalten bei Störungen und Datenschutzverstößen

Kulzer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit von Personenbezogenen Daten, Meldepflicht bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

Bei einer Störung der Verarbeitung oder einer Datenschutzverletzung leitet der unverzüglich alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen Personen und für den Auftraggeber und Verantwortlichen ein.

Kulzer verpflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der Personenbezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz Personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit Personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die Betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können sowie Fälle der Pfändung, Beschlagnahme, Insolvenz- oder Sanierungsverfahren oder sonstige Maßnahmen Dritter. Zu den Datenschutzverstößen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne des MSA und dieser ADV.

Der Auftraggeber muss Kulzer unverzüglich über jeden möglichen Missbrauch seiner Konten oder Authentifizierungsdaten oder jedes Sicherheitsproblem im Zusammenhang mit der Nutzung seiner Dienstleistungen benachrichtigen.

Die Partei, die für die Verletzung des Schutzes Personenbezogener Daten verantwortlich ist, muss unverzüglich eine Untersuchung der Verletzung des Schutzes Personenbezogener Daten vornehmen und die andere Partei über den Fortschritt der Untersuchung auf dem Laufenden halten sowie angemessene Maßnahmen ergreifen, um die Folgen weiter zu minimieren. Beide Parteien erklären sich einverstanden, im Rahmen dieser Untersuchungen uneingeschränkt zu kooperieren und sich gegenseitig bei der Einhaltung etwaiger Benachrichtigungserfordernisse und -verfahren zu unterstützen.

Die Verpflichtung einer Partei, eine Verletzung des Schutzes Personenbezogener Daten zu melden oder darauf zu reagieren, kann nicht und wird nicht als Eingeständnis eines Fehlers oder einer Haftung im Hinblick auf die Verletzung des Schutzes Personenbezogener Daten durch diese Partei ausgelegt werden.

§ 11 Weisungsbefugnis des Auftraggebers

Der Kulzer verarbeitet die Personenbezogenen Daten nur nach Weisung des Auftraggebers. Der Auftraggeber kann jederzeit über Art, Umfang und Verfahren der Datenverarbeitung bestimmen. Solche Weisungen sind stets schriftlich zu erteilen. Soll der Verarbeitungsgegenstand oder das generelle Verfahren zur Datenverarbeitung geändert werden, so ist dies zwischen den Parteien gemeinsam abzustimmen.

Kulzer informiert den Auftraggeber unverzüglich, falls er der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Bis zur Bestätigung oder Änderung der problematischen Weisung durch den Auftraggeber, ist Kulzer berechtigt, die Weisung auszusetzen.

§ 12 Löschung und Rückgabe von Personenbezogenen Daten

Nach Wegfall aller in Art 6 DSGVO genannten Berechtigungen wird Kulzer die übermittelten Daten zunächst anonymisieren und unbeschadet etwaiger Back-up-Archive spätestens sechs (6) Monate nach Erlöschen der Rechtfertigungen nach Art. 6 DSGVO löschen oder auf Wunsch des Auftraggebers diesem übersenden und in keinem Fall weiter nutzen.

Auf schriftliche Anfrage des bestätigt Kulzer die Löschung schriftlich.

§ 13 Haftung

Die Parteien haften gegenüber betroffenen Personen sowie untereinander entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§ 14 Datenschutzbeauftragter

Kulzer hat gem. Art. 37 DSGVO einen Datenschutzbeauftragten bestellt, welcher Überwachung der Einhaltung der datenschutzrechtlichen Anforderungen sowie die Zusammenarbeit mit den Datenschutzaufsichtsbehörden koordiniert.

Die Kontaktdaten des Datenschutzbeauftragten lauten:

Kulzer GmbH

Data Privacy Officer

Leipziger Straße 2

63450 Hanau

e-mail: legal@kulzer-dental.com

§ 15 Geheimhaltung

Die Parteien vereinbaren, dass sämtliche Daten, die im Rahmen des Vertrages aus dem Geschäftsbereich der jeweils anderen Partei bekannt werden, als „vertraulich“ behandelt werden und über die Laufzeit des Vertrages hinaus die Geheimhaltungspflicht hinsichtlich dieser Daten gewahrt wird. Kulzer wahrt insoweit auch die Geheimhaltungsverpflichtung des Auftraggebers oder Verantwortlichen als Berufsträger.

§ 16 Diverses

Diese Vereinbarung ersetzt alle etwaigen bereits bestehenden Datenschutzvereinbarungen. Gerichtsstand für sämtliche Streitigkeiten aus dieser Vereinbarung ist Hanau.

Anhang 1: Einzelheiten zur Verarbeitung von Personenbezogenen Daten

I. Betroffene Personen. Im Rahmen der Vertragserfüllung des MSA werden personenbezogene Daten folgender Kategorien betroffener Personen durch Kulzer verarbeitet:

- Auftraggeber ggfls. Verantwortlicher
- Arbeitnehmer des Auftraggebers/Vertragspartners/Verantwortlichen
- Patienten des Auftraggebers/Vertragspartners/Verantwortlichen

II. Kategorien Personenbezogener Daten. Die Vertragserfüllung kann die Verarbeitung der folgenden Kategorien Personenbezogener Daten umfassen: Namen, Adressen, Kontaktdaten (E-Mail, Telefonnummern), Vertragsdaten, Gesundheitsdaten.

III. Verarbeitungszwecke. Die übermittelten personenbezogenen Daten betreffen alle relevanten Informationen, die zur Erbringung der Dienstleistungen erforderlich sind, einschließlich der folgenden Datenkategorien

- Vertragsdurchführung, inkl. Service- und Informationsdienstleistungen
- Forschung & Entwicklung
- Statistische Zwecke

IV. Unterauftragnehmer. Kulzer bedient sich folgender Kategorien von Unternehmen zur Vertragsdurchführung:

- Zahntechniker
- Hardware/Software-Support
- Informationsdienstleister

Anhang 2: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Folgende technische und organisatorische Maßnahmen sind eingerichtet und gelten als vereinbart:

Zugangskontrolle

Es werden individuelle Benutzer und Passwörter erstellt.

Das Passwort muss beim ersten Einloggen und spätestens alle 90 Tage vom Berechtigten selbst geändert werden.
Folgende Passwortregeln gelten:

- Beim Einrichten eines Benutzers wird ein Initial-Passwort vergeben. Dieses muss bei der ersten Anmeldung geändert werden.
- Das Passwort muss mindestens 8 Stellen haben und mindestens 3 der 4 folgenden Komplexitätskriterien erfüllen: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen
- Nach 90 Tagen läuft das Passwort ab und muss geändert werden.
- Nach 10 erfolglosen Anmeldeversuchen wird der Benutzer gesperrt. Die Entsperrung erfolgt durch das zuständige IT Service Desk oder über den Kulzer Passwort Self Service.
- Nach 15 Minuten ohne Eingabe sperrt sich der Bildschirm. Zum Entsperren ist eine Passworteingabe erforderlich.

Zutrittskontrolle

Zutritt zu den Geschäftsräumen wie auch zu den Servern haben nur Mitarbeiter von Kulzer sowie Dienstleister, denen sich Kulzer zur Erfüllung des Geschäftszwecks bedient.

Der Zugang zu den Unternehmensräumen ist mit einem elektronischen Zugangskontrollsystem gesichert. Die Mitarbeiter erhalten eine Zugangskarte, die bei Verlust gesperrt wird. Die Zutrittskarten werden sofort eingezogen, wenn der Mitarbeiter aus dem Dienstverhältnis ausscheidet.

Die Zugänge in das Bürogebäude sind videoüberwacht. Weiterhin ist der Eingang des Werksgeländes sowie der Bürogebäude von Personal beaufsichtigt.

Das Gebäude ist durch eine Alarmanlage gesichert.

Der Zugang zum Serverstandort ist durch Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten gesichert. Darüber hinaus sind technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung getroffen worden.

Zugriffskontrolle

Die Authentifikation erfolgt über Benutzername und Passwort. Hierdurch erhält jeder Mitarbeiter nur Zugriff auf die Daten, die für seine Funktion notwendig sind.

Der Benutzeraccount wird sofort gesperrt, wenn die Berechtigung erlischt, beispielsweise bei Ausscheiden eines Mitarbeiters oder bei Wegfall von Berechtigungen.

Alle Internetzugänge sind durch Firewalls abgesichert. Default Ports nach außen: http; https; ftp; smtp; dns. Default Ports nach innen: smtp; dns; Default Ports in DMZ: http; https; ftp; smtp; dns

Der Zugriff auf interne Dienste erfolgt ausschließlich über geeignete Sicherheitseinrichtungen wie Reverse Proxy Lösungen, die dem aktuellen Stand der Technik entsprechen. ·eitere Ports werden nur auf Anforderung und nach vorhergehender Sicherheitsanalyse und Freigabe durch die Kulzer IT geöffnet.

Trennungskontrolle

Getrennte Systeme für unterschiedliche Aufgaben.

Getrennte Datenbanken je Anwendung auf die mit unterschiedlicher Berechtigung zugegriffen werden kann.

Weitergabekontrolle

Alle Datenverbindungen auf das Kulzer Netzwerk über das Internet werden verschlüsselt. Dies gilt sowohl für Netzwerkanbindungen (Kulzer-VPN) als auch für die Anbindung von mobilen Endgeräten (Netscaler, O365). Der Verschlüsselungsgrad ist entsprechend dem aktuellen Stand der Technik pro IT-Service festgelegt

Zum Versenden und Empfangen von vertraulichen Mails stellt Kulzer IT eine zentrale Lösung – basierend auf dem Verschlüsselungsstandard S/MIME – zur Verfügung.

Nicht mehr benötigte Datenträger und Fehldrucke werden datenschutzgerecht entsorgt. Datenträger werden vor der Vernichtung durch den Dienstleister gelöscht.

Datenträgern auf mobilen Geräten (Mobiltelefone, Laptops, mobile Festplatten) sind verschlüsselt.

Eingabekontrolle

Änderungen an Daten, Anwendungen und Systemen werden protokolliert mit Datum, Uhrzeit, User und welche Daten es betrifft. Dies betrifft auch Administrator-Tätigkeiten.

Die Protokolldaten werden gespeichert und gesondert gegen Verlust oder Veränderung gesichert.

Verfügbarkeitskontrolle

Kulzer ergreift zum Schutz der Daten vor zufällige oder mutwillige Zerstörung folgende Mittel:

Backup-Verfahren

Es gibt ein Backup- und Recoverykonzept. Im Falle eines Zwischenfalls kann die letzte Datensicherung wiederhergestellt werden.

Unterbrechungsfreie Stromversorgung (USV) mit gesteuertem Herunterfahren bei niedriger Restladung von Akkus

Virenschutz (zentral verwaltet)

Firewall

Klimaanlagen

Brandmeldeanlage

Alarmanlage

Auftragskontrolle

Sämtliche Dienstleister, die Kulzer zur Erfüllung des MSA nutzt, sind durch schriftliche Verträge zur Auftragsdatenverarbeitung verpflichtet, die hier festgelegten Grundsätze einzuhalten.

Alle zugriffsbefugten Mitarbeiter sind auf das Datengeheimnis und die Vertraulichkeit verpflichtet.

Schulungen zu datenschutzrechtlichen Themen sowie zum Umgang mit vertraulichen Informationen finden regelmäßig statt.

Ein Datensicherheitskonzept hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz liegt vor.

Datenschutz-Management

Interne Richtlinien, u.a. zum Umgang mit personenbezogenen Daten und vertraulichen Informationen sowie zur allgemeinen Betriebssicherheit sind in Kraft

Führung eines Datenverarbeitungsverzeichnisses aller relevanter Vorgänge

Incident-Response-Management

Schulung aller Mitarbeiter zum Umgang bei Datenverletzungen und Störungen, insbesondere die Verpflichtung, diese umgehend zu melden

Monitoring von IT-Systemen

Einrichtung einer IT-interne Sicherheitsorganisation, die u.a. mit der Bewertung von Sicherheitsvorfällen, Sicherheitslücken und Risiken und der Bewertung neuer IT-Sicherheitsanforderungen beraut ist.