Vertrag zur Auftragsverarbeitung
Zahntechnik

Zwischen

Auftraggeber (Verantwortlicher):

Name	
Adresse	(Straße, PLZ, Ort)

und

Auftragnehmer (Auftragsverarbeiter):

Name	**creacam frästechnik gmbh & co.kg**
Adresse	**Am Campus 15** **48712 Gescher**

wird folgende Vereinbarung getroffen:

1. Gegenstand

Der Auftraggeber lässt beim Auftragnehmer im Rahmen von Werkverträgen Zahnersatz für seine Patienten herstellen. Der Auftragnehmer verarbeitet dabei personenbezogene Daten der Patienten des Auftraggebers im Sinne der Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.
Zusätzlich leistet der Auftragnehmer bei Bedarf Support beim Auftraggeber via Fernwartungssoftware. Hierbei schaltet sich der Auftragnehmer auf das System des Auftraggebers. Ggf. erhält er hierdurch Einsicht in personenbezogene Daten des Patienten.

Die vertraglich vereinbarte Werkleistung wird ausschließlich in Deutschland und damit 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 Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. Dauer

Die Dauer der Auftragsverarbeitung ergibt sich aus dem erteilten Auftrag.
Ohne Einhaltung einer Frist kann der Auftraggeber jederzeit den Vertrag kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

3. Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die Überlassung der personenbezogenen Daten der Patienten erfolgt ausschließlich zur Erstellung und Abrechnung von Zahnersatz durch den Auftragsnehmer. Bei den überlassenen Daten handelt es sich um den Namen und das Geburtsdatum des Patienten, seinen Versicherungsstatus sowie die erforderlichen Behandlungsinformationen (z.B. Abdrücke, Modelle, Therapieplanung). Von der Datenüberlassung sind damit Gesundheitsdaten betroffen.

Während Supportleistungen via Fernwartungssoftware erfolgt ggf. eine Einsicht in personenbezogene Daten des Patienten (Auftragsdaten / Daten, die im Fräsprogramm hinterlegt sind). Eine weitergehende Speicherung und anderweitige Verarbeitung erfolgt im Zuge der Wartung nicht.

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

5. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Beim Auftraggeber ist weisungsberechtigt:

Name	
Telefon	
E-Mail	

Weisungsempfänger beim Auftragnehmer:

Name	Michael Borghorst
Telefon	0 25 42 / 91 75 95 0
E-Mail	daten@creacam.de

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertretermitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

6. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28

Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Nachweis von Maßnahmen zum Datenschutz und zu Datensicherung, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen (z.B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.). Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragte/r für den Datenschutz bestellt:

Adresse	ITM systems GmbH & Co. KG Datenschutzbeauftragte - creacam Hauptstraße 43 48712 Gescher
Telefon	02542 917 918 0
E-Mail	datenschutz@itm-systems.com

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

7. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. § 4 dieses Vertrages durchführen.

8. Unterauftragsverhältnisse (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art.

32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage 1 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

9. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird (die aktuell eingesetzten Maßnahmen des Auftragnehmers sind Anlage 2 zu entnehmen).

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzkonform zu vernichten.

11. Hinweis auf § 203 StGB

Sofern der Auftraggeber der Schweigepflicht gem. § 203 StGB unterliegt: Der Auftragnehmer bestätigt, dass er vom Auftragnehmer auf die strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht, insbesondere über § 203 StGB, hingewiesen wurde. Der Auftragnehmer hat seine Mitarbeiter oder Subunternehmer zur Verschwiegenheit zu verpflichten und anzuhalten, soweit sie in Erfüllung dieser Vereinbarung für den Auftraggeber tätig werden, und auf die strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht, insbesondere über § 203 StGB, hinzuweisen. Der Auftragnehmer hat Subunternehmer zu verpflichten, dass diese ihre Mitarbeiter zur Verschwiegenheit verpflichten und

auf die strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht, insbesondere auf § 203 StGB, hinzuweisen.

12. Haftung

Auf Art. 82 DSGVO wird verwiesen.

13. Sonstige Vereinbarungen

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Gescher, 01.07.2022	_____, _____
Ort, Datum	Ort, Datum
	
_____	_____
Unterschrift Auftragnehmer	Unterschrift Auftraggeber

Anlage 1 – Unterauftragsverhältnisse

Sofern für die Auftragsabwicklung erforderlich, erhalten wir Unterstützung durch die folgenden Subunternehmen.

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**
W.B. Zahntechnik am Campus GmbH & Co. KG	Am Campus 15 48712 Gescher Deutschland	Tätigkeit als Dentallabor (Erstellung von Zahnersatz, Kronen, Brücken etc.)
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen Deutschland	Software zur Durchführung von Fernwartung
Henry Schein Dental Deutschland GmbH	Monzastr. 2a 63225 Langen Deutschland	Maschinen-Hersteller, Durchführung von (Fern-)Wartung / Support an der Maschine
DATRON AG	In den Gänsäckern 5 64367 Mühltal Deutschland	Maschinen-Hersteller, Durchführung von (Fern-)Wartung / Support an der Maschine
Dental Concept Systems GmbH	Gieselwerder Str. 2 37194 Wahlsburg Deutschland	Maschinen-Hersteller, Durchführung von (Fern-)Wartung / Support an der Maschine
DSJ Dental Solutions Jade (UG)	An der Junkerei 48E 26389 Wilhelmshaven Deutschland	Maschinen-Hersteller, Durchführung von (Fern-)Wartung / Support an der Maschine
ENVISIONTEC GMBH	Brüsseler Straße 51 45968 Gladbeck Deutschland	3D-Drucker-Hersteller, Durchführung von (Fern-)Wartung / Support
CIMT GmbH	Hinter dem Hamberge 34 37124 Rosdorf Deutschland	Maschinen-Hersteller, Durchführung von (Fern-)Wartung / Support an der Maschine
ESCOdent GmbH	Westring 49 33818 Leopoldshöhe Deutschland	Software-Anbieter / Durchführung von (Fern-)Wartung
ITM systems GmbH & Co. KG	Hauptstraße 43 48712 Gescher Deutschland	IT-Dienstleister / Wartung, Support bzgl. des IT-Systems
X-Team Bocholt GmbH & Co. KG	Dinxperloer Str. 65 46399 Bocholt Deutschland	IT-Dienstleister / Wartung von Multifunktionsgeräten

Anlage 2 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch:

- Absicherung von Gebäudeschächten
- elektronisches Schließsystem mit Schließautomatik
- Zutrittsautorisierung (Mitarbeiterausweise mit gespeicherten Zutrittsberechtigungen inkl. Lichtbild)
- manuelles Schließsystem
- besetzter Empfang
- Aufenthalt von betriebsfremden Personen nur in Begleitung von Mitarbeitern

Serverraum:

- Zutritt zum Serverraum geregelt, zutrittsberechtigte Personen namentlich benannt
- Arbeit im Serverraum durch Fremdpersonal wird von zutrittsberechtigten Personen beaufsichtigt
- Serverraum und Serverschrank verschlossen (Sicherheitsschloss, Zugang zum Flur mit Kartensystem verschlossen)

Zugangskontrolle

Keine unbefugte Systembenutzung durch:

- Authentifikation mit individuellem Benutzernamen / Passwort
- Organisatorische Passwortrichtlinie
- Automatische, passwortgeschützte Rechnersperre
- Verschlüsselung von Datenträgern
- Zuordnen von Benutzerprofilen zu IT-Systemen
- Regelung für die Löschung von Berechtigungen ausgeschiedener Mitarbeiter
- Verbindliches Verfahren zur Vergabe von Berechtigungen
- Einsatz von Anti-Viren-Software
- Sicherung interner Netze gegen unberechtigte Zugriffe von extern (Firewall)
- Externer Zugriff auf interne Netze durch VPN-Technologie

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

- Dokumentation der Berechtigungen
- Einsatz von Aktenvernichtern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Protokollierung und datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
- Unwiederbringliche Löschung von Daten auf Datenträgern, insb. vor deren Wiederverwendung, sofern erforderlich
- Ausreichender Zugriffsschutz / sichere Aufbewahrung auf / von Datenträger/n
- Alle Mitarbeiter sind zur Vertraulichkeit (Art. 23 Abs. 3 S.2 lit. b DSGVO) und auf die Weisungsgebundenheit (Art. 29 DSGVO) verpflichtet
- Protokollierung von Zugriffen

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch:

- Logische Mandantentrennung
- Berechtigungskonzept mit Festlegung der Zugriffsrechte

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. Umgesetzt durch:

- Verwendung von Patientennummern anstelle von Klarnamen

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

- Zugriff auf personenbezogene Daten nur über authentifizierte Kanäle
- Dokumentation von Datenempfängern bei Transport oder Übermittlung
- Dokumentation der Abruf- und Übermittlungsprogramme (im Verfahrensverzeichnis)
- Bei physischem Transport sichere Transportbehälter/-verpackungen

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch:

- Übersicht, mit welchen Applikationen Daten eingegeben, geändert oder gelöscht werden können (im Verfahrensverzeichnis)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden.
- Löschungsregelung für Protokolldaten (Löschkonzept)

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

- Notfallkonzept bei IT-Störungen vorhanden
- Redundante Absicherung von Daten und Datenbeständen
- Unterbrechungsfreie Stromversorgung (USV) in Serverräumen
- Automatische Feuer- und Rauchmeldeanlagen
- CO2-Löscher in unmittelbarer Näher zum Serverraum
- Sicherungs- und Wiederherstellungskonzept von Daten
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort

- Rekonstruktion von Datenbeständen und Test der Datenbestände
- Einsatz von Virenscannern / Abwehr von Schadsoftware
- Automatisierte Aktualisierung von Virenscannern / Anti-Malware
- Richtlinie zur Wartung und Durchführung von Updates & Upgrades
- Automatisches und permanentes Monitoring zur Erkennung von Störungen sowohl informationstechnischer als auch infrastruktureller Art durch einen IT-Dienstleister
- Durchführung von Penetrationstests

Belastbarkeit

Sicherstellung der Belastbarkeit der Systeme und Dienste durch:

- Es werden regelmäßige Belastungstest durchgeführt und deren Ergebnis dokumentiert.
- Einsatz von Load Balancing zur Verteilung der Last auf Servern/-farmen
- Einsatz von Load Balancing zur Verteilung der Last in Netzwerkstrukturen (WAN / LAN)

Rasche Wiederherstellbarkeit

Fähigkeit zur raschen Wiederherstellung personenbezogenen Daten nach einem physischen oder technischen Zwischenfall durch:

- Es wird ein IT-Notfallhandbuch eingesetzt, das regelmäßig aktualisiert und auf dem neusten Stand gehalten wird.
- Es wird regelmäßig eine Wiederherstellung (Recovery) relevanter Anwendungen getestet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch:

- Datenschutz-Management
- Es besteht eine Richtlinie im Rahmen des Datenschutzmanagementsystems, die die regelmäßige Durchführung, Bewertung und Evaluierung der technisch organisatorischen Maßnahmen festlegt.
- Incident-Response-Management
- Bestellung eines Datenschutzbeauftragten
- Es werden regelmäßig Audits durchgeführt und dokumentiert, um die Beachtung und Umsetzung der Richtlinie im Unternehmen zu prüfen.
- Das DSMS wird als Plan-Do-Check-Act Regelkreis umgesetzt und nach Audit erkannte Defizite werden behoben.

Datenschutz als Standard

- Datenschutzfreundliche Voreinstellungen – Das Prinzip aus Art. 25 DSGVO Privacy by default wird umgesetzt mit Unterstützung eines IT-Dienstleisters.
- Datenschutz durch Technikgestaltung – Das Prinzip aus Art. 25 DSGVO Privacy by design wird umgesetzt mit Unterstützung eines IT-Dienstleisters.

Auftragskontrolle

- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers
- Verpflichtung auf Vertraulichkeit
- Eindeutige Vertragsgestaltung

- formalisiertes Auftragsmanagement
- strenge Auswahl des Dienstleisters
- Kontrolle der Datensicherheitsvorkehrungen durch Prüfung einer entsprechenden Dokumentation / Zertifizierungsnachweisen