HENRY SCHEIN®
DENTAL

Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DSGVO

Die vorliegende Vereinbarung zur Datenverarbeitung im Auftrag **(„Vereinbarung“)** wird geschlossen zwischen:

(1) _____
Vertragspartner (z.B. Arzt, Dentallabor, etc.), Geschäftsanschrift

– „Verantwortlicher“ –

Henry Schein Dental Kundennummer: _____

und

(2) Henry Schein Dental Austria GmbH, Schönbrunner Straße 297, 1120 Wien

– „Verarbeiter“ –

– Verantwortlicher und Verarbeiter jeweils einzeln „**Partei“**, gemeinsam **„Parteien“** –

Präambel

A. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien und bezieht sich auf alle Tätigkeiten, bei denen der Verarbeiter und seine Mitarbeiter oder durch ihn beauftragte Dritte mit Personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

B. Diese Vereinbarung gilt für die Verarbeitung von Personenbezogenen Daten im Sinne der EU-Datenschutzgrundverordnung 2016/679 („DSGVO“) und verwendet die dort genannten Begrifflichkeiten, u.a.:

„Personenbezogene Daten“	sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („Betroffene Person“) beziehen.
„Identifizierbar”	ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
„Verarbeitung”	bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personen- bezogenen Daten. Das betrifft u.a. und nicht abschließend, 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.

1. Verarbeitung durch den Verarbeiter

1.1. Zweck der Verarbeitung: Der Verarbeiter erbringt für den Verantwortlichen folgende Dienstleistungen: Wartung und Pflege von IT-Systemen des Auftraggebers (einschließlich Fernwartung und Vor-Ort- Einsatz) hinsichtlich Software und Hardware/Technik sowie Einweisung bzw. Training in Bezug auf: IT-Infrastruktur (allgemein); Patientenverwaltungssystem (PVS) Software; Röntgendiagnoseprogramme; CAD/CAM Software, Dokumentationssoftware Hygiene; Backupsoftware und Antivirus.

1.2. Der Verarbeiter verarbeitet dazu die in folgender Tabelle genannten Arten Personenbezogener Daten zum genannten Zweck von Kategorien Betroffener Personen. Dies betrifft alle relevanten Informationen, die zur Erbringung der Dienstleistung erforderlich sind, einschließlich der folgenden:

Kategorien Personenbezogener Daten	Betroffene Personen
• Persönliche Angaben bzw. Personenstammdaten (z.B. Name, Geburtsdatum, Position, Kundennummer, etc.) • Kontaktdaten (z.B. E-Mail-Adresse, Telefonnummer, etc.) • Vertragsdaten (z.B. Konditionen, Interessen, Historie, etc.) • Authentifizierungsdaten (z.B. Login, ID, IP-Adresse, etc.) • Zahlungs- bzw. Abrechnungsdaten, inkl. Bankdaten • Beschäftigtendaten (z.B. Name, Abwesenheit, etc.) • Sozialdaten (z.B. Versicherung, Behindertengrad, etc.) • Gesundheitsdaten (z.B. Befunde, Diagnosen, etc.) • _____	• Praxis-/Laborinhaber Mitarbeiter • Patienten Kunden Lieferanten Ansprechpartner • Externe IT-Dienstleister des Verantwortlichen • _____ • _____

2. Laufzeit der Vereinbarung

Diese Vereinbarung gilt unbefristet und kann von beiden Parteien mit einer Frist von einem Monat gekündigt werden. Das Recht zur außerordentlichen Kündigung bleibt hiervon unberührt.

3. Verantwortlichkeit und Weisungen

3.1. Der Verantwortliche ist gemäß Art. 4 Ziff. 7 DSGVO für die Rechtmäßigkeit der Datenverarbeitung verantwortlich, einschließlich der Bestimmung von Umfang, Zweck und Art und Weise. Er kann im Rahmen der gesetzlichen Bestimmungen u.a. Berichtigung, Sperrung, Löschung oder Herausgabe von Personenbezogenen Daten verlangen. Der Umgang mit Personenbezogenen Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Verantwortlichen. Die Funktion des Verarbeiters beschränkt sich auf die Verarbeitung im Auftrag.

3.2. Der Verantwortliche wird dem Verarbeiter die für die Verarbeitung relevanten Daten zur Verfügung stellen und sie entsprechend angemessen kennzeichnen. Der Verantwortliche ist berechtigt, seine Weisungen jederzeit schriftlich zu ändern, zu ergänzen oder zu ersetzen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

3.3. Der Verarbeiter kann den Verantwortlichen informieren, wenn eine Weisung seines Erachtens gegen gesetzliche Regelungen, einschließlich Datenschutzvorschriften verstößt. Der Verarbeiter ist berechtigt, die Durchführung dieser Weisung solange auszusetzen, bis sie durch den Verantwortlichen geprüft und ggf. geändert wurde. Hält der Verantwortliche seine, nach Ansicht des Verarbeiters rechtswidrige Weisung aufrecht, stellt er den Verarbeiter sowie ggf. Unterbeauftragte von etwaigen Schäden, die sich aus der konkreten Weisung ergeben, frei.

4. Unterbeauftragung und Verarbeitung in einem Drittland

4.1. Der Einsatz von Unterbeauftragten zur Verarbeitung ist gestattet, soweit es für die Erfüllung dieser Vereinbarung oder gesetzlich notwendig ist. Unterbeauftragten müssen die gleich wirkenden datenschutzrechtlichen Pflichten auferlegt werden, wie in dieser Vereinbarung festgelegt, insbesondere im Hinblick auf Vertraulichkeit, technische und organisatorische Maßnahmen („TOM“) sowie Kontrollrechte. Der Verantwortliche kann den Verarbeiter schriftlich um Auskunft hinsichtlich der Pflichten der Unterbeauftragten bitten.

4.2. Der Verarbeiter wählt Unterbeauftragte gewissenhaft aus. Der Verantwortliche kann einer Unterbeauftragung widersprechen. Ein Widerspruch kann jedoch dazu führen, dass die Leistungen des Verarbeiters nicht erfolgreich erbracht werden können. Hierzu werden sich die Parteien im Falle des Falles besprechen.

4.3. Der Verarbeiter wird die vertraglichen Leistungen in Deutschland oder einem Mitgliedsstaat der EU oder des EWR – soweit die EU mit diesen Staaten Vereinbarung darüber erzielt hat, dass die DSGVO entsprechende Anwendung findet - bzw. in den Standorten der Unterbeauftragten erbringen.

4.4. Findet eine Leistungserbringung in einem Land statt, das kein Mitgliedsstaat der EU oder ein sogenannter „sicherer Drittstaat“ ist, wird der Verarbeiter für die Einhaltung der besonderen Voraussetzungen der Art. 44 ff. DSGVO (Übermittlung personenbezogener Daten an Drittländer) Sorge tragen.
D.h. der Verarbeiter ist verantwortlich dafür, dass die Datenübermittlung auf rechtmäßiger Grundlage erfolgt, z.B.:

a) auf der Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO),

b) durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2b), 47 DSGVO),

c) durch den Einsatz der EU-Standarddatenschutzklauseln, die von der Kommission erlassen werden (Art. 46 Abs. 2c) DSGVO), oder

d) eine sonstige in Art. 46 Abs. 2 DSGVO beschriebene geeignete Garantie.

5. Technische und organisatorische Maßnahmen

5.1. Der Verarbeiter gestaltet seine interne Organisation so, dass Personenbezogene Daten des Verantwortlichen nach den besonderen Anforderungen des Datenschutzes vor Missbrauch und Verlust geschützt sind. Er gewährleistet insbesondere die Sicherheit der Verarbeitung (Art. 28 Abs. 3, 32 DSGVO). Dies betrifft u.a. die Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten sowie die Art, der Umfang und die Zwecke der Verarbeitung, aber auch unterschiedliche Eintrittswahrscheinlichkeiten und die angenommene Schwere des jeweiligen Risikos für die Rechte und Freiheiten der Betroffenen Personen zu berücksichtigen.

5.2. Anlage 5.2 legt die TOM fest, die der Verarbeiter zur Sicherung und zum Schutz der Personenbezogenen Daten vor- und einhält. Auf schriftliche Anfrage wird er sie dem Verantwortlichen und gegebenenfalls der zuständigen Aufsichtsbehörde gegenüber nachweisen. Der Verarbeiter kontrolliert regelmäßig seine internen Prozesse sowie die TOM, um die Verarbeitung im Einklang mit geltendem Datenschutzrecht und den Schutz der Rechte der Betroffenen Person zu gewährleisten. Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Verarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen, soweit dadurch das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und der Verantwortliche ist zu informieren. Eine Änderung dieser Anlage gilt nicht als Vertragsänderung im Sinne von Ziffer 12.3.

6. Weitere Pflichten des Verarbeiters, Qualitätssicherung

Der Verarbeiter hat die gesetzlichen Pflichten gemäß Artt. 28 bis 33 DSGVO zu gewährleisten. Das betrifft insbesondere:

6.1. Zweckbindung: Der Verarbeiter und jede ihm unterstellte Person, inkl. Unterbeauftragte, die Personenbezogene Daten verarbeitet, darf dies nur im Rahmen dieser Vereinbarung tun, es sei denn, das Recht der EU oder Mitgliedstaaten bestimmt eine andere Verarbeitung.

6.2. Datenschutzbeauftragte/r: Der Verarbeiter hat einen Datenschutzbeauftragten (Art. 38 f. DSGVO) bestellt. Dieser ist per E-Mail unter: datenschutz@henryschein.at erreichbar. Weitere Kontaktdaten sowie etwaige Veränderungen werden dem Verantwortlichen auf Anfrage unverzüglich mitgeteilt. Dies gilt nicht als Vertragsänderung im Sinne von Ziffer 12.3.

6.3. Datengeheimnis/Wahrung der Vertraulichkeit: Der Verarbeiter setzt für die Verarbeitung nur Personen ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Sie müssen darauf hingewiesen werden, dass das Datengeheimnis ggf. auch nach Beendigung der Tätigkeit fortbestehen kann. Eine gesetzliche Offenbarungspflicht des Verarbeiters bleibt hiervon unberührt.

Dem Verarbeiter ist bekannt, dass er zur Verschwiegenheit über Geheimnisse (Art. 2 § 6 DSG), die ihm im Rahmen seiner Tätigkeit bekannt werden, verpflichtet ist, und dass diese Verpflichtung auch nach Beendigung dieser Vereinbarung gilt. Er wird die von ihm zur Erfüllung dieser Vereinbarung beschäftigten Personen und ggf. Unterbeauftragte über den Regelungsgehalt des Art. 2 § 6 DSG sowie die Folgen einer Pflichtverletzung informieren und entsprechende Verschwiegenheit einfordern.

7. Fernzugriff zur Prüfung oder Wartung

Für die Durchführung von sogenannten Fernzugriffen zu Prüfungs- oder Wartungsarbeiten von Datenverarbeitungsanlagen durch den Verarbeiter („Remote Access-Maßnahmen“), z.B. von Rechnern oder Systemen des Verantwortlichen gilt:

7.1. Remote Access-Maßnahmen an Arbeitsplatzsystemen werden erst nach Freigabe des Verantwortlichen bzw. seiner Mitarbeiter, z. B. durch Anklicken einer Pop-Up-Box auf dem Rechner, durchgeführt.

7.2. Remote Access-Maßnahmen an automatisierten Verfahren oder Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf Personenbezogene Daten nicht ausgeschlossen werden kann, grundsätzlich, soweit z.B. nicht Gefahr im Verzug ist, nur mit Zustimmung des Verantwortlichen ausgeführt.

7.3. Falls notwendig werden sich Verarbeiter und Verantwortlicher vor Durchführung von Remote Access-Maßnahmen über etwaig notwendige Datensicherungsmaßnahmen in ihrem jeweiligen Verantwortungsbereich verständigen.

7.4. Der Verarbeiter verwendet angemessene Identifizierungs- und Verschlüsselungsverfahren und wird von den eingeräumten Zugriffsrechten nur in dem Umfang Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der Remote Access-Maßnahme notwendig ist.

7.5. Remote Access-Maßnahmen werden dokumentiert und protokolliert. Der Verantwortliche ist soweit technisch möglich berechtigt, die Remote Access-Maßnahmen vor, während und nach Durchführung zu verfolgen, zu kontrollieren und jederzeit abzubrechen.

7.6. Soweit eine Fehleranalyse erforderlich ist, die eine Kenntnisnahme (z.B. lesender Zugriff) oder einen Zugriff auf oder einen Abzug von Produktivbetriebsdaten (Produktions-/Echtdaten) des Verantwortlichen z.B. auf mobile Speichermedien wie externe Festplatten, USB-Sticks, etc. notwendig macht, wird der Verarbeiter die Zustimmung einholen. Bei Datenabzug wird der Verarbeiter alle Kopien nach Bereinigung des Fehlers vom verwendeten Speichermedium löschen. Produktivbetriebsdaten dürfen nur zum Zweck der Fehleranalyse verarbeitet werden.

7.7. Remote Access-Maßnahmen sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung der TOM zum Schutz Personenbezogener Daten durchgeführt.

8. Pflichten des Verantwortlichen

8.1. Der Verantwortliche ist im Hinblick auf die zu verarbeitenden Personenbezogenen Daten für die Einhaltung der jeweils einschlägigen Datenschutzgesetze selbständig verantwortlich. Dies gilt insbesondere hinsichtlich Personenbezogener Daten seiner Mitarbeiter, Patienten bzw. Kunden, für die zur Verarbeitung eingesetzten automatisierten Verfahren sowie bezüglich seiner Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten (Verfahrensverzeichnis). Dem Verantwortlichen obliegen weiterhin
z.B. die aus den Artt. 33, 34 DSGVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde oder Betroffenen Personen.

8.2. Der Verantwortliche wird den Verarbeiter unverzüglich umfassend informieren, wenn er bei der Prüfung der Verarbeitungstätigkeiten Fehler oder Unregelmäßigkeiten im Hinblick auf Bestimmungen des Datenschutzes oder dieser Vereinbarung feststellt.

8.3. Nach Beendigung der Zusammenarbeit legt der Verantwortliche die Maßnahmen zur Rückgabe überlassener Datenträger oder Löschung von gespeicherten Personenbezogenen Daten fest.

8.4. Der Verantwortliche ist auch nach Ende der Zusammenarbeit verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Verarbeiters vertraulich zu behandeln.

9. Zusammenarbeit und Information

9.1. Die Parteien arbeiten bei Anfragen von Betroffenen Personen oder der Aufsichtsbehörden zusammen. Soweit Betroffene Personen sich unmittelbar an den Verarbeiter wenden, wird er dies unverzüglich an den Verantwortlichen weiterleiten. Ist der Verantwortliche aufgrund geltender Datenschutzregelungen verpflichtet, z.B. Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Personenbezogenen Daten zu geben, wird der Verarbeiter den Verantwortlichen nach schriftlicher Aufforderung angemessen unterstützen.

9.2. Der Verarbeiter unterstützt den Verantwortlichen bei der Einhaltung der datenschutzrechtlichen Pflichten zur Sicherheit Personenbezogener Daten, zur Meldepflicht bei Datenverstößen, bei Datenschutz-Folgeabschätzungen und Konsultationen (Artt. 32 bis 36 DSGVO). Hierzu gehören jeweils im Rahmen der rechtlichen Bestimmungen, u.a. die:

a) Sicherstellung eines angemessenen Schutzniveaus durch TOM, einschließlich der sofortigen Feststellung relevanter Verletzungsereignisse,

b) Meldung von Verletzungen Personenbezogener Daten,

c) Unterstützung im Zusammenhang mit Informationspflichten gegenüber Betroffenen Personen,

d) Unterstützung in Angelegenheiten gegenüber Aufsichtsbehörden.

9.3. Der Verarbeiter wird den Verantwortlichen im Rahmen der Gesetze über eigene und über Datenschutzverstöße der durch ihn beschäftigten Personen informieren. Das gilt entsprechend bzgl. etwaiger Kontrollen oder anderer Maßnahmen der Aufsichtsbehörde beim Verarbeiter, soweit es sich auf die Verarbeitung von Personenbezogenen Daten nach dieser Vereinbarung oder allgemein auf den Verantwortlichen bezieht. Falls notwendig, trifft er die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen Personen und spricht sich hierzu mit dem Verantwortlichen ab.

9.4. Soweit der Verantwortliche einer Kontrolle einer Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, einem Haftungsanspruch einer Betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Verarbeitung nach dieser Vereinbarung ausgesetzt ist, wird ihn der Verarbeiter angemessen unterstützen.

9.5. Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Verarbeiters zurückzuführen sind, kann dieser eine Erstattung des tatsächlich entstandenen Aufwands beanspruchen.

10. Überprüfungen

10.1. Der Verantwortliche kann sich auf eigene Kosten selbst oder durch Einbindung qualifizierter und zur Verschwiegenheit verpflichteter Dritter, die nicht in einem Wettbewerbsverhältnis zum Verarbeiter stehen („Prüfer“), von der Einhaltung der vereinbarten Regelungen überzeugen. Mittels Stichprobenkontrollen, die stets ausreichend rechtzeitig vorher anzumelden sind und den Geschäftsbetrieb des Verarbeiters nicht unangemessen beinträchtigen dürfen, kann sich der Verantwortliche von der Einhaltung dieser Vereinbarung durch den Verarbeiter in dessen Geschäftsbetrieb überzeugen.

10.2. Der Verarbeiter wird dem Verantwortlichen oder dem Prüfer auf schriftliche Anforderung alle notwendigen Auskünfte erteilen und ggf. die Umsetzung der TOM nachweisen, z.B. durch Vorlage aktueller Testate, Berichte oder Auszüge unabhängiger Instanzen.

11. Löschung und Rückgabe Personenbezogener Daten

11.1. Der Verarbeiter erstellt grundsätzlich keine Kopien oder Duplikate der Daten ohne Wissen des Verantwortlichen, soweit es nicht Datensicherung oder Kopien betrifft, die zur Verarbeitung oder für sonstige Tätigkeiten nach dieser Vereinbarung erforderlich sind. Eine Berichtigung oder Löschung Personenbezogener Daten durch den Verarbeiter erfolgt grundsätzlich nur nach Anweisung des Verantwortlichen oder zur Einhaltung gesetzlicher Pflichten.

11.2. Nach Ende dieser Vereinbarung oder nach schriftlicher Anweisung des Verantwortlichen vor Ende dieser Vereinbarung wird der Verarbeiter nach eigener Wahl sämtliche Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Verarbeitung stehen, dem Verantwortlichen aushändigen oder vernichten. Nach schriftlicher Aufforderung übersendet der Verarbeiter dem Verantwortlichen eine Bestätigung der Löschung.

11.3. Ungeachtet des Vorstehenden hat der Verarbeiter gegebenenfalls gesetzliche Aufbewahrungsfristen oder entsprechende Pflichten zur Speicherung zu beachten, d.h. Dokumentationen etc. sind gegebenenfalls auch nach Vertragsende weiter aufzubewahren, insbesondere soweit sie dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung dienen.

12. Sonstige Regelungen

12.1. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Rechtslage nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Bestimmungen und die Wirksamkeit der Vereinbarung im Ganzen hiervon unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll eine wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der unwirksamen oder undurchführbaren Bestimmung möglichst nahekommt. Für den Fall der fehlenden Regelung in dieser Vereinbarung gilt die Bestimmung als vereinbart, die dem Sinn und Zweck der Vereinbarung entspricht und die man im Falle des Bewusstseins des Fehlens vereinbart hätte.

12.2. Im Falle des Konflikts zwischen Regelungen dieser Vereinbarung und seiner Anlagen geht die Regelung dieser Vereinbarung vor.

12.3. Änderungen und Ergänzungen dieser Vereinbarung, einschließlich - soweit nicht anders geregelt - Anlagen, bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

12.4. Es gilt österreichisches Recht. Gerichtsstand ist der Sitz des Verarbeiters.

Henry Schein Dental Austria GmbH	
	Vertragspartner (z.B. Arzt, Dentallabor, etc.)
Wien im Juni 2024	
Ort, Datum	Ort, Datum
Unterschrift	Unterschrift
Roman Reichholf, Geschäftsführer	
Name, Funktion (in Druckbuchstaben)	Name, Funktion (in Druckbuchstaben) ggf. Stempel

Anlage 5.2 – Technisch-Organisatorische Maßnahmen (TOM) gemäß DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1b DSGVO)

a. Zutrittskontrolle:
- Manuelles Schließsystem, Sicherheitsschlösser, elektrische Türöffner, autom. Zugangskontrollsystem, Magnet- oder Chipkarten-/Transponder-Schließsystem,
- Videoüberwachung der Zugänge, Videoanlagen, Absicherung von Gebäudeschächten, Bewegungsmelder,
- Personenkontrolle beim Empfang, Protokollierung der Besucher, Werkschutz, Pförtner,
- Schlüsselregelung (Schlüsselausgabe, etc.)
- Sorgfältige Auswahl von Reinigungs- und Wachpersonal, Tragepflicht von Berechtigungsausweisen

b. Zugangskontrolle:
- Kennwörter, autom. Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zuordnung / Erstellen von Benutzerrechten und -profilen
- Passwortvergabe gemäß PW-Richtlinie (Länge / Wechsel), Authentifikation mit Benutzername/Passwort,
- Gehäuseverriegelungen
- Einsatz von Virtual Private Networks-Technologie
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Smartphone-Inhalten
- Zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Hard-/Software Firewalls, Anti-Viren-Software

c. Zugriffskontrolle:
- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, inkl. Festlegung von Datenbankrechten
- Verwaltung der Rechte durch System-Admins
- Anzahl der System-Admins auf Notwendigstes reduziert
- Protokollierung von Zugriffen auf Anwendungen, insb. bei Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757); Einsatz von versierten Aktenvernichtern bzw. Dienstleistern; Protokollierung der Vernichtung

d. Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:
- Mandantenfähigkeit und logische Mandantentrennung (softwareseitig)
- Sandboxing; physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern; Trennung von Produktiv- und Testsystem
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

e. Pseudonymisierung (Artt. 32 Abs. 1a, 25 Abs. 1 DSGVO): Soweit anwendbar und gesetzlich notwendig: Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung weiterer Informationen nicht mehr einer spezifischen Person zugeordnet werden können (wenn weitere Informationen gesondert aufbewahrt
werden und entsprechenden TOM unterliegen.

2. Integrität (Art. 32 Abs. 1b DSGVO)

a. Weitergabekontrolle:
- Einrichtungen von Standleitungen bzw. Virtual Private Networks-Tunneln
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

b. Eingabekontrolle:
- Berechtigungskonzepte bzgl. und Protokollierung von Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Dokumentenmanagement, Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

3. Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1b DSGVO)

a. Schutz zufälliger/m oder mutwilliger/m Zerstörung/ Verlust:
- Unterbrechungsfreie Stromversorgung
- Meldewege, Notfallpläne, Temperatur-/ Feuchtigkeitsüberwachung, Schutzsteckdosen-leisten in Serverräumen
- Feuer- und Rauchmeldeanlagen; automatische Löschanlage in Serverräumen, bzw. Feuerlöscher am äußeren Eingangsbereich von Serverräumen
- Alarm bei unberechtigten Zutritten zu Serverräumen
- Serverräume nicht unter sanitären Anlagen und über der Wassergrenze
- Virenschutz, Firewall

b. Wiederherstellbarkeit (Art. 32 Abs. 1c DSGVO):
- Backup-Strategie: Erstellen eines Backup- & Recoverykonzepts (online/offline; on-site/off-site)
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artt. 32; 25 DSGVO)

a. Datenschutz-Management
b. Incident-Response-Management
c. Datenschutzfreundliche Voreinstellungen
d. Auftragskontrolle / Weisungsgebundenheit:
- Auswahl des Verarbeiters oder Sub-Verarbeiters unter DSGVO-Sorgfaltsgesichtspunkten
- Eindeutige Vertragsgestaltung, z.B. durch DSGVO konforme Auftragsverarbeitungsvereinbarung
- Dokumentation der TOM sowie Kontrollrechte.
- Verpflichtung der Mitarbeiter des Dienstleisters auf das Datengeheimnis
- soweit gesetzlich verpflichtet hat Dienstleister Datenschutzbeauftragten bestellt
- Überprüfung des Dienstleisters und seiner Tätigkeiten
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags