Vertrag zur Auftragsverarbeitung mit Wartung von IT-Systemen

Vereinbarung

zwischen

Auftraggeber eintragen mit Kontaktdaten

Dr. Georg Linford

Bahnhofstraße 28
19077 Rastow

Verantwortlicher (nachstehend Auftraggeber genannt)

und

Datenschutzbeauftragter der Praxis

Auftragsverarbeiter (nachstehend Auftragnehmer genannt)

synMedico GmbH

Wilhelmshöher Allee 300

34131 Kassel

Allgemeines/Begriffsbestimmung:

Zwischen den Parteien besteht ein Vertragsverhältnis über die Wartung und/oder Pflege von IT-Systemen (Leistungsvereinbarung). Die vorliegende Vereinbarung wird als ergänzende Einhaltung der datenschutzrechtlichen Vorgaben der Datenschutzgrundverordnung insb. des Art. 28 DGSVO geschlossen.

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen und durchführen zu können.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der zwischen den Parteien geschlossenen Leistungsvereinbarung über die Wartung und/oder Pflege von IT-Systemen vom *01.05.2018*

auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

1.2. Dauer

Dieser Vertrag gilt ab seiner Unterzeichnung.

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom *Datum eintragen*

oder

☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Installation und Systemwartung

2.2. Anforderungen an das Schutzniveau bei internationalen Auftragsverarbeitungen
(nur auszufüllen, wenn Verarbeitungen außerhalb der EU stattfinden)

Jede Verlagerung der vertraglich vereinbarten Datenverarbeitungen in ein Drittland (kein Mitgliedsstaat der Europäische Union oder Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum) erfordert grundsätzlich der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen an das Schutzniveau der Artt. 44 ff. DS-GVO erfüllt sind.

Das angemessene Schutzniveau in

(hier bitte entsprechendes Drittland eintragen)

☐	ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO)	☐	wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO)
☐	wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO)	☐	wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO)
☐	Wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO)	☐	wird hergestellt durch folgende sonstige Maßnahmen (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO) *bitte Maßnahmen eintragen*

2.3 Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: *bitte angeben*

oder

☒ Während der Wartungs- und Pflegearbeiten kann nicht ausgeschlossen werden, dass der Auftragnehmer Zugriff auf folgende Datenarten/-kategorien erhält: (Aufzählung/Beschreibung der Datenkategorien)

☒	Personenstammdaten	☐	Vertragsabrechnungs- und Zahlungsdaten
☒	Kommunikationsdaten (z.B. Telefon, E-Mail)	☐	Planungs- und Steuerungsdaten

☐	Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)	☐	Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐	Kundenhistorie	☐	Mitarbeiterstammdaten
☐	Kundendaten	☐	Logistikdaten
☒	Patientenstammdaten	☒	Patientenbefunddaten
☒	Kommunikationsdaten	☐	Sonstige Datenarten: *bitte beschreiben*

2.4 Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: *bitte angeben*

oder

☒ Die Kategorien der durch die Verarbeitung möglicherweise betroffenen Personen umfassen:

☒	Kunden	☐	Lieferanten
☐	Interessenten	☐	Handelsvertreter
☐	Abonnenten	☐	Ansprechpartner
☒	Beschäftigte	☒	Patienten
☐	Sonstige:		

2.5 Fernwartung

(1) Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(2) Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

(3) Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken, solange das Vertragsverhältnis zwischen Auftragnehmer und Auftraggeber besteht. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.
(3) Nach Ende des Vertragsverhältnisses ist der Auftragnehmer verpflichtet sämtliche personenbezogene Daten, die während der Dauer des Vertrages erhoben wurden, zu löschen und diese Löschung zu dokumentieren.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

☒ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☒ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau *[Fa. deData GmbH & Co KG., Herr Ron Wieland, wieland@dedata.de, 0561/3168589]* bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☒ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau *bitte eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail* benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union:
Bitte eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten

ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 1).

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) 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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgend genannten Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

d) ☒ der Wechsel des bestehenden Unterauftragnehmers
sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☒ ist nicht gestattet;

Unterauftragnehmer:	Anschrift:	Leistung
Bitte Firmenname eintragen	*Bitte Anschrift eintragen*	*Bitte Leistung eintragen*
Bitte Firmenname eintragen	*Bitte Anschrift eintragen*	*Bitte Leistung eintragen*

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, 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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Kassel, 02.06.2021	Kassel, den 01.05.2018
Ort, Datum	Ort, Datum
02.06.2021, 12:40:18 (MESZ)	
- Auftraggeber -	- Auftragnehmer –

synMedico

Anlage zu Technisch-organisatorischen Maßnahmen

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

1.1 Zutrittskontrollmaßnahmen

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☒	Alarmanlage	☒	Absicherung v. Gebäudeschächten
☒	Automatisches Zugangskontrollsystem	☒	Chipkarten-/Transponder-Schließsystem
☐	Schließsystem mit Codesperre	☐	Manuelles Schließsystem
☐	Biometrische Zugangssperren	☒	Videoüberwachung der Zugänge
☐	Lichtschranken / Bewegungsmelder	☒	Sicherheitsschlösser
☒	Schlüsselregelung (Schlüsselausgabe etc.)	☒	Personenkontrolle beim Pförtner / Empfang
☒	Protokollierung der Besucher	☒	Sorgfältige Auswahl von Reinigungspersonal
☐	Sorgfältige Auswahl von Wachpersonal	☒	Tragepflicht von Berechtigungsausweisen
☐	Sonstige Maßnahmen:		

1.2 Zugangskontrollmaßnahmen

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

☒	Zuordnung von Benutzerrechten	☒	Erstellen von Benutzerprofilen
☒	Passwortvergabe	☐	Authentifikation mit biometrischen Verfahren
☒	Authentifikation mit Benutzername / Passwort	☒	Zuordnung von Benutzerprofilen zu IT-Systemen
☒	Gehäuseverriegelungen	☒	Einsatz von VPN-Technologie
☐	Sperren von externen Schnittstellen (USB etc.)	☒	Sicherheitsschlösser
☒	Schlüsselregelung (Personalabteilung, Serverraum, Archive etc.)	☒	Verwendung von elektronischen Schließsystemen
☒	Protokollierung der Zugänge (Serverraum, Personalabteilung, Archive)	☒	Einsatz von Intrusion-Detection-Systemen
☒	Verschlüsselung von mobilen Datenträgern	☒	Verschlüsselung von Smartphone-Inhalten
☐	Einsatz von zentraler Smartphone-Administrations-Software	☒	Einsatz von Anti-Viren-Software
☒	Verschlüsselung von Datenträgern in Laptops / Notebooks	☐	Einsatz einer Hardware-Firewall
☒	Einsatz einer Software-Firewall	☐	Sonstige Maßnahmen: *bitte beschreiben*

1.3 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

1.4 Zugriffskontrollmaßnahmen

Maßnahmen, die gewährleisten, dass die Benutzer eines Datenverarbeitungssystems ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☒	Erstellen eines Berechtigungskonzepts	☒	Verwaltung der Rechte durch Systemadministrator
☒	Anzahl der Administratoren auf das „Notwendigste“ reduziert	☒	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☒	Protokollierung von Zugriffen auf Anwendungen, insb. bei der Eingabe, Änderung und Löschung von Daten	☒	Sichere Aufbewahrung von Datenträgern
☒	physische Löschung von Datenträgern vor Wiederverwendung	☒	ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
☒	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)	☒	Protokollierung der Vernichtung
☒	Verschlüsselung von Datenträgern	☐	Sonstige Maßnahmen:

1.5 Trennungsgebot

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

☐	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
☒	Erstellung eines Berechtigungskonzepts	☐	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
☒	Versehen der Datensätze mit Zweckattributen/Datenfeldern	☒	Logische Mandantentrennung (softwareseitig)
☒	Festlegung von Datenbankrechten	☒	Trennung von Produktiv- und Testsystem
☐	Sonstige Maßnahmen:		

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

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☒	E-Mail-Verschlüsselung	☒	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
☐	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	☐	Beim physischen Transport: sichere Transportbehälter/-verpackungen
☒	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -Fahrzeugen	☒	Logische Mandantentrennung (softwareseitig)
☐	Sonstige Maßnahmen: *bitte beschreiben*		

2.2 Eingabekontrolle

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

☒	Protokollierung der Eingabe, Änderung und Löschung von Daten	☒	Erstellen einer Übersicht darüber, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
☒	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	☐	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☐	Sonstige Maßnahmen: *bitte beschreiben*		

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

3.1 Verfügbarkeitskontrolle

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

☒	Unterbrechungsfreie Stromversorgung (USV)	☒	Klimaanlage in Serverräumen
☒	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☒	Schutzsteckdosenleisten in Serverräumen
☒	Feuer- und Rauchmeldeanlagen	☒	Feuerlöschgeräte in Serverräumen
☒	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	☒	Erstellen eines Backup- & Recoverykonzepts
☒	Testen von Datenwiederherstellung	☒	Erstellen eines Notfallplans
☒	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	☒	Serverräume nicht unter sanitären Anlagen
☒	In Hochwassergebieten: Serverräume über der Wassergrenze	☐	Sonstige Maßnahmen: *bitte eintragen*

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

4.1 Auftragskontrolle

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

☒	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	☐	vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
☒	schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)	☐	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (Mit Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen)
☒	Auftragnehmer hat Datenschutzbeauftragten bestellt	☐	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart	☐	laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
☐	Vertragsstrafen bei Verstößen	☐	Sonstige Maßnahmen:

Zeitliches Erstellungsprotokoll

Aktionen im Arztmodus

02.06.2021, 11:46:28: Formular 'ADV Vertrag' geöffnet
02.06.2021, 11:46:41: Textfeld IDF_BEHANDLUNGSEINRICHTUNG_NAME1 editiert
02.06.2021, 11:46:54: Textfeld IDF_BEHANDLUNGSEINRICHTUNG_STREET editiert
02.06.2021, 11:47:07: Textfeld IDF_BEHANDLUNGSEINRICHTUNG_ZIPCITY editiert
02.06.2021, 12:40:07: Weiter auf 'Seite 2'
02.06.2021, 12:40:07: Weiter auf 'Seite 3'
02.06.2021, 12:40:08: Weiter auf 'Seite 4'
02.06.2021, 12:40:08: Weiter auf 'Seite 5'
02.06.2021, 12:40:08: Weiter auf 'Seite 6'
02.06.2021, 12:40:09: Weiter auf 'Seite 7'
02.06.2021, 12:40:10: Weiter auf 'Seite 8'
02.06.2021, 12:40:12: Weiter auf 'Seite 9'
02.06.2021, 12:40:14: Weiter auf 'Seite 10'
02.06.2021, 12:40:19: In 'Unterschrift_NP' unterschrieben
02.06.2021, 15:58:41: 'Seite 1' aus dem Dokument aufgerufen