Anlage – Vertrag über eine Auftragsverarbeitung gemäß Art. 28. Datenschutz-Grundverordnung (DS-GVO)

(Online-Produkte Gesundheitsfachberufe)

Präambel

Im Rahmen der Nutzung des OnlineCenter verarbeitet die NOVENTI HealthCare GmbH (nachfolgend: „Auftragnehmer“) personenbezogene Daten im Auftrag des Kunden (nachfolgend: „Auftraggeber“). Um die Rechte und Pflichten aus diesem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DS-GVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1. Gegenstand des Auftrags, Art und Zweck der Verarbeitung und Dauer der Auftragsverarbeitung

1.1. Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich aus der zwischen den Parteien geschlossenen Vereinbarung über die Nutzung des OnlineCenters und über die Nutzung der zusätzlich durch den Auftraggeber gebuchten Produkte im OnlineCenter unter den Webseiten www.azh-onlinecenter.de, http://www.srz-onlinecenter.de oder www.zrk-onlinecenter.de einschließlich der Nutzungsbedingungen (nachfolgend: „Nutzungsvereinbarung“). Soweit der Auftraggeber den Auftragnehmer mit der Übernahme von Dienstleistungen im Rahmen des elektronischen Kostenvoranschlags (eKV) beauftragt hat, sind die maßgebliche Grundlage für die Ausführung dieser Dienstleistungen durch den Auftragnehmer die Regelungen der §§ 300, 302 SGB V und § 105 SGB XI und alle damit in Zusammenhang stehenden gesetzlichen Bestimmungen und vertraglichen Vereinbarungen, die die Berufs- und Interessenverbände der Leistungserbringer auf Bundes- und Landesebene mit Rechtswirkung für ihre Mitglieder oder die der Auftraggeber selbst abgeschlossen haben („Annexverträge“).

1.2. Der Auftraggeber übermittelt dem Auftragnehmer im Rahmen des Nutzungsvertrages personenbezogene Daten („Daten“). Diese werden nur im Auftrag und nach Weisung des Auftraggebers gemäß Art. 28 DS-GVO (Auftragsverarbeitung) und den nachfolgenden Bestimmungen verarbeitet.

1.3. Die Laufzeit dieser Auftragsdatenvereinbarung („Vereinbarung“) entspricht der Laufzeit der Nutzungsvereinbarung zwischen Auftraggeber und Auftragnehmer.

1.4. Im Rahmen der Auftragsverarbeitung werden die folgenden personenbezogenen Daten verarbeitet:

1.5. Abhängig von der Art des vom Kunden gebuchten Abrechnungs- bzw. Finanzierungsprodukts werden die folgenden personenbezogenen Daten verarbeitet:

- Alle erforderlichen Daten gemäß der jeweils aktuellen Version der technischen Anlage 3 und Anlage 4 zur Vereinbarung zur Datenübermittlung nach § 300 SGB V
- Alle erforderlichen Daten gemäß der jeweils aktuellen Version der Anlage 1 der technischen Anlage für die maschinelle Abrechnung (elektronische Datenübermittlung) zu den Richtlinien der Spitzenverbände der Krankenkassen nach § 302 Abs. 2 SGB V
- Alle erforderlichen Daten gemäß der jeweils aktuellen Fassung der technischen Anlage 3 zur Regelung der Datenübermittlung nach § 105 Abs. 2 SGB XI
- ggf. weitere personenbezogene Daten gemäß den technischen Anlagen zu den §§ 300 und 302 SGB V oder § 105 SGB XI.
- Im Fall der Buchung des Produkts „CashDirekt“ alle erforderlichen Daten für die vereinbarte (reine) Vorfinanzierung
- Im Fall der Buchung des Produkts „KVCheck“ alle im Kostenvoranschlag enthaltenen Daten (Verordnungsdaten, Versorgungsdaten, Name und Kontaktdaten des Leistungserbringers).

1.6. Unabhängig von der Art des vom Kunden gebuchten Abrechnungs- bzw. Finanzierungsprodukts werden die folgenden personenbezogenen Daten verarbeitet:

- Versichertenstamm: Name, Geburtsdatum, Anschrift, Versichertennummer
- Arztstamm: Arzt-/Praxisname, Anschrift Arztpraxis, BSNR
- Herstellerstamm: Name, Anschrift
- Daten des Auftraggebers (Leistungserbringer): Name, Anschrift, elektronische Nachrichten des Auftraggebers oder an den Auftraggeber
- Gesundheitsdaten

1.7. Kreis der betroffenen Personen:

- Auftraggeber
- Kunden der Auftraggeber bzw. Patienten
- Ärzte, Leistungserbringer
- Beschäftigte bei Leistungserbringern, Lieferanten und Leistungsträgern

2. Datensicherheit

2.1. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die datenschutzrechtlichen Bestimmungen (DS-GVO, BDSG, SGB) eingehalten werden. Das sind insbesondere die notwendigen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung dauerhaft sicherstellen, wie auch
- • dafür sorgen, dass die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen unterhalten, damit die Sicherheit der Verarbeitung gewährleistet ist.

2.2. Dabei ist der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen (nach Art. 32 Abs. 1 DS-GVO) zu berücksichtigen.

2.3. Die technisch- organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, entsprechende Alternativen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen der technisch-organisatorischen Maßnahmen wird der Auftragnehmer dem Auftraggeber über das elektronische Postfach des Auftraggebers im OnlineCenter mitteilen.

3. Unterstützungspflichten des Betroffenen

3.1 Der Betroffene unterstützt unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten.

3.2 Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DS-GVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DS-GVO).

4. Berichtigung, Sperrung und Löschung von Daten

4.1. Der Auftragnehmer hat die Daten, die im Auftrag verarbeitet werden, nur nach Weisung des Auftraggebers zu

berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich direkt an den Auftragnehmer zur Berichtigung oder Löschung seiner Daten wendet, wird dieser das Ersuchen sofort an den Auftraggeber weiterleiten. Bei Beauftragung unterstützt der Auftragnehmer den Auftraggeber soweit möglich und vereinbart. Der Auftragnehmer haftet nicht, wenn der Auftraggeber die Aufforderung der betroffenen Person nicht, nicht richtig oder nicht fristgerecht beantwortet.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat folgende Pflichten aus Art. 28 DSGVO:

5.1. Schriftliche Bestellung eines Datenschutzbeauftragten: Kontaktdaten: Berg-am-Laim-Straße 105, 81673 München, E-Mail: datenschutz@noventi.healthcare

5.2. Verpflichtung der Mitarbeiter auf die Vertraulichkeit: Gemäß Art. 28 Abs. 3 S. 2 lit. b DS-GVO sowie gemäß § 35 Abs. 1 SGB I sind alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf die Vertraulichkeit sowie das Sozialgeheimnis verpflichtet. In diesem Zusammenhang sind die Mitarbeiter und Subauftragnehmer – soweit erforderlich – unter Berücksichtigung von § 203 StGB verpflichtet. Sie wurden auch über die bestehende Weisungs- bzw. Zweckbindung belehrt. Diese Verpflichtung besteht auch nach Beendigung des Auftrages fort.

5.3. Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen.

5.4. Durchführung der Auftragskontrolle: Der Auftragnehmer prüft regelmäßig die Vertragsausführung bzw. -erfüllung, insbesondere die Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur entsprechenden Durchführung.

5.5. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber.

5.6. Unterstützung des Auftraggebers mit den vorhandenen Informationen zur Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO, sowie bei vorheriger Beratung mit der zuständigen Aufsichtsbehörde nach Art. 36 DS-GVO.

6. Unterauftragsverhältnisse

6.1. Die Auslagerung auf Unterauftragnehmer oder der Wechsel bestehender Unterauftragnehmer ist zulässig, soweit

6.1.1. der Auftragnehmer den Auftraggeber über eine solche Auslagerung mit angemessenem zeitlichem Vorlauf in Textform informiert und

6.1.2. der Auftraggeber nicht binnen 14 Tagen ab Zugang der Information in Textform Einspruch gegen die geplante Auslagerung erhebt.

6.2. . Für diese Unterauftragnehmer gilt die Genehmigung für das Tätigwerden als erteilt. Über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmers wird der Auftragnehmer den Auftraggeber durch eine Nachricht über das elektronische Postfach des Auftraggebers im OnlineCenter informieren.

6.3. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und dem Auftragnehmer entsprechen. Der Auftraggeber muss beim Unterauftragnehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung erhalten.

6.4. Keine Unterauftragsverhältnisse sind Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung für die Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer muss jedoch auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen treffen sowie Kontrollmaßnahmen ergreifen, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

7. Kontrollrechte des Auftraggebers

7.1. Der Auftraggeber hat das Recht, die in Art. 28 Abs. 3 Satz 2 lit. h) DS-GVO vorgesehene Auftragskontrolle in Absprache mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer vornehmen zu lassen. Er hat das Recht, sich durch Stichproben, die in der Regel rechtzeitig angemeldet werden müssen, davon zu überzeugen, dass diese Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb eingehalten wird. Der Prüfer darf nicht in unmittelbarem Wettbewerbsverhältnis mit dem Auftragnehmer stehen. Die Kontrollen dürfen nicht zu übermäßigen Beeinträchtigungen des Geschäftsablaufs führen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise zur Verfügung zu stellen.

7.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen mit geeigneten Mitteln nach.

8. Mitteilungen bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer informiert in allen Fällen den Auftraggeber, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen, um die Daten zu sichern und mögliche nachteilige Folgen für die Betroffenen einzudämmen. Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich nach gesicherter Kenntnis eines meldepflichtigen Vorfalls zu informieren (d. h. insbesondere über die Ursachen, den genauen Zeitpunkt sowie das Ausmaß), damit der Auftraggeber die erforderlichen Maßnahmen treffen kann (z. B. Meldung bei der zuständigen Aufsichtsbehörde). Die Information über einen meldepflichtigen Vorfall erfolgt durch eine entsprechende Mitteilung des Auftragnehmers in das elektronische Postfach des Auftraggebers im OnlineCenter.

8.2. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DS-GVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

8.3. Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen, damit dieser seine Informationspflicht wie folgt erfüllen kann:

8.3.1. gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DS-GVO und

8.3.2. ggf. gegenüber den Betroffenen, bei denen der Schutz der personenbezogenen Daten gemäß Art. 34 DS-GVO verletzt wurde.

9. Weisungsbefugnis des Auftraggebers

9.1. Der Umgang mit den Daten erfolgt ausschließlich nach der zwischen den Parteien geschlossenen Nutzungsvereinbarung und nach in Textform gefasster Weisung des Auftraggebers. Ausnahmen sind eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Sollte eine anderweitige Verpflichtung bestehen, teilt der Auftragnehmer dem Auftraggeber unverzüglich die entsprechenden rechtlichen Anforderungen noch vor der Verarbeitung mit.

9.2. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger in Textform erfolgter Zustimmung durch den Auftraggeber erteilen. Ausgeschlossen sind Auskünfte zu denen der Auftragnehmer gesetzlich oder vertraglich (Nutzungsvereinbarung) verpflichtet ist.

9.3. Mündliche Weisungen wird der Auftraggeber unverzüglich in Textform bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist nicht berechtigt, sie an Dritte weiterzugeben.

9.4. Der Auftragnehmer muss den Auftraggeber unverzüglich informieren, wenn er der Meinung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9.5. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Dies gilt nicht, wenn diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie bei Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten benötigt werden.

9.6. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DS-GVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44-49 DS-GVO erfüllt sind.

10. Löschung von Daten und Rückgabe von Datenträgern

10.1. Nach Abschluss der vertraglichen Arbeiten – spätestens mit Beendigung der Nutzungsvereinbarung – muss der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, oder Kopien, die das Auftragsverhältnis betreffen, dem Auftraggeber aushändigen oder nach vorheriger Zustimmung datenschutzgerecht vernichten und löschen oder anonymisieren. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen

10.2. Dokumentationen, Unterlagen und Datenbestände, zu deren Aufbewahrung der Auftragnehmer gesetzlich sowie vertraglich für einen längeren Zeitraum verpflichtet ist oder nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dürfen nicht gelöscht werden. Nach Ablauf der gesetzlichen Aufbewahrungspflichten muss der Auftragnehmer die Daten innerhalb eines Monats datenschutzkonform vernichten oder anonymisieren.

10.3. Zurückbehaltungsrechte des Auftraggebers in Bezug auf die personenbezogenen Daten sind ausgeschlossen.

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO (Anlage 1 zum Vertrag über eine Auftragsverarbeitung gemäß Art. 28. Datenschutz-Grundverordnung (DS-GVO) (Online-Produkte Gesundheitsfachberufe)

1. Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 **Zutrittskontrolle** Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.	Zutreffend (falls ja, bitte ankreuzen)
Schließsystem/ Schließanlage	☒
Sorgfältige Auswahl externer Wachdienst	☒
Alarmanlage	☒
Verbindung Alarmanlage zu Wachdienst/ Polizei	☒
Lichtschranken/ Bewegungsmelder	☒
Verbindung Bewegungsmelder zu Wachdienst/ Polizei	☒
Videoüberwachung im NOVENTI Rechenzentrum Tomannweg 6, München	☒
Biometrische Zutrittskontrolle	☐
Wachdienst vor Ort/ Sicherung außerhalb der Arbeitszeiten	☒
Personenüberprüfung bei Pförtner /Empfang	☐
Berechtigungsausweise	☒
Besucherausweise	☒
Protokollierung von Besucherzutritten / Besucherbuch	☒
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☒
Elektronische Zutrittscodekarten/ Zutrittstransponder	☒
Schlüsselregelung	☒
Zutrittsberechtigungskonzept	☒
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	☒
Gesicherter Eingang für An- und Ablieferungen	☒
Gesondert gesicherter Zutritt zum Serverraum	☒
Gesondert gesicherter Zutritt zum Rechenzentrum	☒
Arbeitsanweisungen /Richtlinien bzgl. des Verschließens von Räumlichkeiten bei Verlassen/Arbeitsende	☒
Sorgfältige Auswahl von Reinigungspersonal	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

1.2 **Zugangskontrolle** Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung	Zutreffend (falls ja, bitte ankreuzen)
Zuordnung von Benutzerrechten	☒
Erstellen von Benutzerprofilen	☒
Berechtigungsmanagement	☒
Dokumentierter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	☒
Dokumentierter Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	☒
Dokumentierter Prozess zum Rechteentzug bei Austritt von Mitarbeitern	☒
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	☒
Verwendung von individuellen Passwörtern	☒
Login mit Benutzername und Passwort	☒
Login mit biometrischen Daten	☐
Separates BIOS-Passwort	☒
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	☒
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität:	☒
Mindestens 8 Ziffern	☒
Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 4 Kriterien)	☒
Verhinderung von Trivialpasswörtern (z.B. Passwort1, Passwort2, 123456, qwertz)	☒
Passworthistorie	☐
Verhinderung von PW nach positivem Abgleich mit Wörterbüchern	☐
Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections	☒
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	☒
Angemessen sicheres Verfahren zum Zurücksetzen von Passwörtern	☒
Sonstiges: (z.B. Nutzung von Fido2)	☐
Hashing von gespeicherten Passwörtern	☒
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)	☐
Verschlüsselung von Netzwerken	☒
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	☒
Sperrung von externen Schnittstellen (z.B. USB)	☐
Programmprüfungs- und Freigabeverfahren bei Neuinstallationen	☒
Verwendung von Intrusion-Prevention-Systemen	☐
Nutzung von VPN-Technologie	☒

Einsatz von Anti-Viren-Software: Server	☒
Einsatz von Anti-Viren-Software: Clients	☒
Einsatz einer Software-Firewall	☐
Einsatz einer Hardware-Firewall	☒
Mobile-Device-Management	☒
Aufbewahrung personenbezogener Daten/Datenträgern in verschließbaren Sicherheitsschränken oder in gesondert gesicherten Räumen	☒
Regelung zum Home Office / zu Telearbeit	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

1.3 **Zugriffskontrolle** Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.	Zutreffend (falls ja, bitte ankreuzen)
Nutzung eines Berechtigungskonzepts	☒
Minimaler Einsatz von Administratoren-Konten	☒
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	☒
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	☒
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	☒
Regelmäßige Überprüfung von Berechtigungen	☒
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	☒
Regelmäßige Auswertung von Protokollen (Logfiles)	☒
Zeitliche Begrenzung von Zugriffsmöglichkeiten	☒
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	☒
Protokollierung von Dateizugriffen	☐
Protokollierung von Dateilöschungen	☐
Protokollierung von Dateiveränderungen	☐
SPAM-Filter	☒
Intrusiondetection (IDS)	☐
Software für das Security Information and Event Management (SIEM)	☐
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	☒
Speicherung von Log-Files auf dediziertem LogFile-Server	☒
Verschlüsselte Speicherung der Daten	☒
verwendete Verschlüsselungsalgorithmen:	☒
AES (128/256 bit)	☒
RSA (1024/2048 bit)	☐
Sonstiges:	☐
Verwendete Hash-Funktion:	☒
SHA2 (256, 384, 512 bit)	☒
SHA3	☒
bcrypt	☐
Andere Verfahren:	☐
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)	☐
Kontrollierte Vernichtung von Daten:	
Shredder (Cross-Cut, mindestens Stufe 3, DIN 66399)	☐
Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	☒
Datenträgerentsorgung - Sichere Löschung von Datenträgern (DIN 66399):	☐
Peter-Gutmann-Algorithmus – 35-faches Überschreiben	☐
Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	☐
Entmagnetisierung durch thermische Zerstörung (Erhitzung der Magnetplattenoberfläche über die Curie-Temperatur der verwendeten Beschichtung hinaus)	☐
Entmagnetisierung mittels eines Degaussers	☐
Sonstiges Vernichtungsverfahren:	☐
Richtlinie zur Datenvernichtung	☒
Clean Desk-Policy	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

1.4 **Auftragskontrolle** Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.	Zutreffend (falls ja, bitte ankreuzen)
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	☒
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☒
Vorabkontrollen beim Auftragnehmer vor Vertragsbeginn	☒
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	☒
Vor-Ort-Kontrollen beim Auftragnehmer	☒
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	☒
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	☒
Auftragnehmer hat Datenschutzbeauftragten benannt	☒
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragnehmer	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

1.5 **Trennungskontrolle**	Zutreffend

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt voneinander zu verarbeiten.	(falls ja, bitte ankreuzen)
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	☒
Physikalische Datentrennung (z.B. unterschiedliche Systeme oder Datenträger)	☐
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	☒
Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)	☒
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	☒
Trennung von Entwicklungs-, Test- und Produktivsystem	☒
Zuordnung von Datensätzen zu Zweckattributen	☐
Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei & Speicherung auf einem anderen System	☐
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

2. Maßnahmen zur Gewährleistung der Integrität

2.1 **Weitergabekontrolle** Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten.	Zutreffend (falls ja, bitte ankreuzen)
Wie werden Daten zwischen Verantwortlichem und Dritten übermittelt?	
VPN-Verbindung	☒
Secure File Transfer Protocol (sftp)	☒
Citrix-Verbindung	☒
E-Mail-Verschlüsselung	☒
SMIME	☐
OpenPGP	☒
E-Mail Versand mit verschlüsselten ZIP-Dateien	☒
Datenaustausch über https-Verbindung	☒
verwendetes Verschlüsselungsprotokoll:	
TLS 1.3	☒
Sonstige Versendungsart: Gem. SGB V	☒
verwendete Verschlüsselungsalgorithmen:	
AES (128/256 bit)	☒
RSA (1024/2048 bit)	☐
Diffie-Hellmann	☐
Sonstiges:	☐
Nutzung von Signaturverfahren	☐
Verwendetes Signaturverfahren:	
RSA	☐
ElGamal	☐
DSA	☐
Sonstige: PGP, eigene	☒
Digitales Signieren von Makros	☐
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	☐
Verschlüsselung vertraulicher Datensätze	☒
Verschlüsselung mobiler Datenträger (z.B. Laptop-Festplatten, externe Festplatten, USB-Sticks)	☒
Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken sowie Mobiltelefonen in Sicherheitsbereiche	☐
Regelung zur Anfertigung von Datensatz-Kopien	☐
Erstellen von Sicherungskopien von Datenträgern, die transportiert werden müssen	☐
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	☒
Direktabholung, Kurierdienst, Transportbegleitung	☒
Vollständigkeits- und Richtigkeitsprüfung	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

2.2 Eingabekontrolle Soll gewährleisten, dass Nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat.	Zutreffend (falls ja, bitte ankreuzen)
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒
Manuelle oder automatisierte Auswertung der Protokolle	☒
Differenzierte Benutzerberechtigungen:	☒
Einzelne Benutzernamen, keine Benutzergruppen	☒
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☒
Feldzugriff bei Datenbanken	☒
Organisatorische Festlegung von Eingabezuständigkeiten	☒
Verpflichtung auf das Datengeheimnis	☒
Über OS-Standard hinausgehendes Log-Konzept	☒
Dezidierter Logserver	☒
Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)	☒
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

3. Maßnahmen zur Gewährleistung der Verfügbarkeit & Belastbarkeit

3.1 **Verfügbarkeitskontrolle** Soll Daten gegen zufällige Zerstörung oder Verlust schützen.	Zutreffend (falls ja, bitte ankreuzen)
Brandmeldeanlagen in Serverräumen	☒
Rauchmelder in Serverräumen	☒
Brandschutztüren an papierverarbeitenden Standorten und im Rechenzentrum	☒
Wasserlose Brandbekämpfungssysteme in Serverräumen	☒
Wassersensoren in Serverräumen - Wasserableitung	☒
Blitz-/ Überspannungsschutz	☒
Klimatisierte Serverräume	☒
Serverräumlichkeiten in separaten Brandabschnitt	☒
Unterbringung von Backupsystemen in separaten Räumlichkeiten und in separatem Brandabschnitt	☒
Serverräume nicht unter oder neben sanitären Anlagen	☒
Zutrittsbegrenzung bei Serverräumen auf notwendiges Personal	☒
Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen	☒
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	☒
CO2-Feuerlöscher in unmittelbarer Nähe der Serverräume	☒
USV-Anlage (Unterbrechungsfreie Stromversorgung)	☒
Stromgenerator	☒
Feuerfeste Schränke	☐
Datenschutztresor	☒
Dokumentiertes Datensicherungs- und Backupkonzept	☒
Durchführung von Datensicherungen und Erstellen von Backups	☒
Regelmäßige Tests zur Datenwiederherstellung	☒
Spiegeln der Festplatten (z.B. RAID)	☒
Getrennte Partitionen für Betriebssystem und Daten	☐
Havariearchiv (Auslagerung von Daten)	☐
Notfallplan vorhanden (BSI-Standard 100-4)	☒
Gewährleistung der langfristigen technischen Lesbarkeit von Backupspeichermedien	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

3.2 Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle) Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.	Zutreffend (falls ja, bitte ankreuzen)
Redundante Stromversorgung	☒
Redundante Datenanbindung	☒
Redundante Klimatisierung	☒
Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?): Hot	☒
sonstige redundante Systeme/Verfahren:	☐
Einsatz einer hochverfügbaren SAN-Lösung (Storage Area Network)	☒
Computer Emergency Response Team (CERT)	☐
Einsatz von Lastenverteilung (Load Balancing)	☒
Abgrenzung kritischer Komponenten	☒
Durchführung von Penetrationstests	☒
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	☒
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	☒
Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)	☒
Prozess zur unverzüglichen Meldung von Vorkommnissen an die IT ist allen Mitarbeitern bekannt	☒
Abschluss einer Cyber-Versicherung	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

4. Cloudlösungen bei Partnerunternehmen

Unsere Partner sind sorgfältig ausgewählt und verfügen über entsprechende Zertifizierungen.

5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.	Zutreffend (falls ja, bitte ankreuzen)
Verarbeitungsverzeichnisse (Art. 30 I und II DSGVO) werden jährlich aktualisiert	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten	☒
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert	☒
Prüfung der Wirksamkeit getroffener Sicherheitsmaßnahmen mind. jährlich	☒
Bei negativen Feststellungen im Rahmen der zuvor gen. Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst	☒
Prozess zur Reaktion auf Sicherheitsverletzungen (Angriffe) und Systemstörungen existiert (Incident-Response-Management)	☒
Dokumentation von Sicherheitsvorfällen	☒
Einsatz Security Intelligence	☒

Sicherheitszertifizierungen (ISO 27001, BSI IT-Grundschutz etc.)	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

5.2 Sonstiges Datenschutzmanagement	Zutreffend (falls ja, bitte ankreuzen)
Einsatz einer Datenschutzmanagement-Software	☒
Datenschutzbeauftragter benannt	☒
IT-Sicherheitsbeauftragter benannt	☒
Dokumentierter Prozess zum Umgang mit Datenschutzvorfällen	☒
Klare Verantwortlichkeiten bei der Handhabung von Datenschutz- und Sicherheitsvorfällen	☒
Zentrale, für alle Mitarbeiter zugängliche Ablage von Richtlinien/Verfahrensanweisungen	☒
Sonstige Maßnahmen: Klicken Sie hier, um Text einzugeben.	☐

Anlage 2 – Unterauftragnehmer
(Anlage 2 zum Vertrag über eine Auftragsverarbeitung gemäß Art. 28. Datenschutz-Grundverordnung (DS-GVO) (Online-Produkte Gesundheitsfachberufe)

Im Zusammenhang mit der Erbringung der vertraglichen Leistungen beauftragt der Auftragnehmer folgende Subunternehmer:

Produkt	**Unterauftragnehmer**	**Aufgabenfeld**
KVCheck	AOK Systems GmbH Kortrijker Straße 1 53177 Bonn	eKV-Verarbeitung
	HMM Deutschland GmbH Eurotec-Ring 10 47445 Moers	eKV-Verarbeitung
	medicomp GmbH Hoheloogstraße 14 67065 Ludwigshafen	eKV-Verarbeitung
	opta data Finance GmbH Berthold-Beitz-Boulevard 514 45141 Essen	eKV-Verarbeitung
	retarus GmbH Aschauer Straße 30 81549 München	Fax-Versand
DHL-Abholung	DHL Express Germany GmbH Heinrich-Brüning-Str. 5 531143 Bonn	Abholung und Transport von Rezepten