Datenschutzbestimmungen zur Auftragsverarbeitung (DB-AV) (AVV i.S.v. Art. 28 Abs. 3 DSGVO)

zum Vertrag zur Abrechnung von Leistungen gemäß § 115f SGB V (Hybrid-DRG) über die Kassenärztliche Vereinigung Berlin (KV Berlin)

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Vertrag zur Abrechnung von Leistungen gemäß § 115f SGB V und den Regelungen zur Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte Dritte („Unterauftragsverarbeiter“) personenbezogene Daten („Daten“) des Verantwortlichen verarbeiten.

§ 1 Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die in der Anlage A aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben.

§ 2 Weisungen der Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in der Anlage A aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

(3) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft mindestens die in der Anlage C aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

(2) Die in der Anlage C aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der

erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten in der Anlage A mit. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

(4) Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

(5) Sofern der Auftragsverarbeiter Daten des Verantwortlichen im Auftrag verarbeitet, die dem Schutzbereich des § 203 StGB bzw. einem Berufsgeheimnis unterliegen, darf der Auftragsverarbeiter nur dann auf derartige Daten zugreifen, soweit dies im Einzelfall erforderlich ist. Der Auftragsverarbeiter verpflichtet sich in diesem Zusammenhang, alle Personen, die im Rahmen der beauftragten Tätigkeit die in Satz 1 genannten Daten verarbeiten, auf die Geheimhaltung nach § 203 StGB zu verpflichten. Dem Auftragsverarbeiter ist bekannt, dass hinsichtlich der Daten, die dem Schutzbereich des § 203 StGB unterliegen, ein Zeugnisverweigerungsrecht nach § 53a StPO besteht. Über die Ausübung des Rechtes auf Zeugnisverweigerung entscheidet der Berufsgeheimnisträger der Verantwortlichen. Dem Auftragsverarbeiter ist bekannt, dass die dem Berufsgeheimnis unterliegenden Daten, die sich im Gewahrsam des Auftragsverarbeiters zur Erhebung, Verarbeitung oder Nutzung befinden, dem Beschlagnahmeverbot des § 97 Abs. 1, 3 StPO unterliegen. Einer Sicherstellung ist zu widersprechen. Der Verantwortliche ist unverzüglich zu informieren, wenn eine Beschlagnahme der Daten zu erwarten ist oder bevorsteht.

§ 5 Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

§ 6 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens drei Wochen im Voraus in Textform über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Einspruchsrechts zu entscheiden mit der Unterrichtung über die geplante Beauftragung zur Verfügung. Die Inanspruchnahme der in der Anlage B zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

(2) Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der

Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Art. 44 ff. DSGVO sicher, indem – sofern erforderlich - geeignete Garantien gemäß Art. 46 DSGVO getroffen werden.

(4) Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standarddatenschutzklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standarddatenschutzklauseln erfüllt sind.

(5) Im Falle des § 6 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standarddatenschutzklauseln durch und stellt diese dem Verantwortlichen auf Anfrage zur Verfügung. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

(6) Der Auftragsverarbeiter hat die Verpflichtung der weiteren mitwirkenden Personen und der Unterauftragsverarbeiter auf die Geheimhaltung gem. § 203 StGB und § 4 Abs. 5 dieses Vertrages sicherzustellen.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen.

(2) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

(3) Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 8 Mitzuteilende Verstöße

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,

- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 9 Beendigung des Auftrags

(1) Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

§ 10 Beitritt zum Vertrag

Diesem Vertrag können mit Zustimmung aller Parteien über eine Beitrittserklärung jederzeit weitere Parteien als Verantwortliche oder als Auftragsverarbeiter beitreten. Zusätzlich zur Beitrittserklärung sind – soweit erforderlich – die Anlagen A bis C auszufüllen. Ab dem Zeitpunkt des Beitritts gelten die beitretenden Parteien als Vertragsparteien dieses Vertrags mit den entsprechend ihrer Bezeichnung bestehenden Rechten und Pflichten.

§ 11 Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Anlage A zum AVV

Auflistung der beauftragten Dienstleistungen und Kontaktdaten des Datenschutzbeauftragten

Gegenstand der Verarbeitung	Abrechnung von Leistungen gemäß § 115f SGB V (Hybrid-DRG) durch den Auftragsverarbeiter.
Art und Zweck der Verarbeitung	Auftragsgemäße Übernahme und ordnungsgemäße Durchführung der Abrechnung von Leistungen nach § 115f SGB V (Hybrid-DRGs) durch u.a. folgende Einzeltätigkeiten: • Entgegennahme und Prüfung der eingereichten Abrechnungen in formaler Hinsicht • Übermittlung der Leistungsanforderung gemäß den gesetzlichen und vertraglichen Regelungen in der jeweils geltenden Fassung an die Krankenkassen in elektronischer Form Überdies sind Art und Zweck der Verarbeitung im Abrechnungsvertrag und den diesen ergänzenden Dokumenten (AGB) festgelegt.
Art der personenbezogenen Daten	Stammdaten, Adressdaten, Kontaktdaten, Praxisdaten, Abrechnungsdaten bzw. Inhalt der abrechnungsrelevanten Aufträge (u.a. konkrete Abrechnungsdaten wie Bankverbindung, Versichertendaten, Behandlungs-, Diagnose- sowie Prozedurdaten) sowie sonstige Daten, die zur Abrechnung der durchgeführten ärztlichen Leistung verarbeitet werden.
Kategorien betroffener Personen	Ärzte, Patienten sowie sonstige Personen, deren Daten Gegenstand der Abrechnungsunterlagen sind.
Dauer der Verarbeitung	Entspricht der Dauer des Abrechnungsvertrages.

Datenschutzbeauftragter des Auftragsverarbeiters	datenschutz nord GmbH, Zweigstelle Berlin-Charlottenburg, Kurfürstendamm 212, 10719 Berlin, office@datenschutz-nord.de

Anlage B zum AVV

Liste der beauftragten Unterauftragsverarbeiter einschließlich der Verarbeitungsstandorte

Unterauftragsverarbeiter	**Verarbeitungsstandort**	**Beschreibung der Verarbeitung**
Kassenärztliche Vereinigung Nordrhein (KVNO)	Tersteegenstraße 9, 40474 Düsseldorf	Bereitstellung (Hosting, Speicherung) und Betrieb der SaaS-Lösung „Hybrid-DRG-Portal“ zur Durchführung der Abrechnungen inkl. Softwarepflege und Produktmanagement

Anlage C zum AVV

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragsverarbeiter mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Die KV Berlin hat im Rahmen der Beauftragung von Unterauftragsnehmern mit diesen Auftragsdatenverarbeitungsvereinbarungen getroffen, die diesen Datenschutzrichtlinien entsprechen. Die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGV der Unterauftragsnehmer entsprechen im Minimum den technischen und organisatorischen Maßnahmen der KV Berlin.

Maßnahmen zur Sicherstellung der Vertraulichkeit und der Integrität

1 Zutrittskontrollmaßnahmen zu Büroräumen					
1.1	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros?				☒ Ja ☐ Nein
1.2	Wird eine Besucherliste geführt?				☒ Ja ☐ Nein
1.3	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?				☐ Ja ☒ Nein
1.4	Wer wird informiert, wenn die EMA auslöst?				*Nur relevant, wenn 1.3 mit ja beantwortet wurde.*
	☐ beauftragter Wachdienst	☐ Administrator	☐ Leiter IT	☐ Sonstiges	
	Bei Sonstiges geben Sie hier entsprechend weitere Informationen ein.				
1.5	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht?				☐ Ja, ohne Bildaufzeichnung ☐ Ja, mit Bildaufzeichnung ☒ Nein
1.6	Wie lange werden die Bilddaten gespeichert? Geben Sie die Dauer in Tagen an. Tage				*Nur relevant, wenn 1.5 mit ja beantwortet wurde.*
1.7	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? ☒ Ja, Gebäude und Büroräume sind elektronisch verschlossen ☐ Ja, aber nur das Gebäude, nicht der Eingang zu den Büros bzw. zur Büroetage. ☐ Ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. ☐ Nein				
1.8	Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!**				*Nur relevant, wenn 1.5 mit ja beantwortet wurde.*
	☒ RFID	☐ PIN	☐ Biometrie	☐ Sonstiges	
	Bei Sonstiges geben Sie hier entsprechend weitere Informationen ein.				
1.9	Werden die Zutrittsrechte personifiziert vergeben?				☒ Ja ☐ Nein
1.10	Werden die Zutritte im Zutrittssystem protokolliert?				*Nur relevant, wenn 1.9 mit ja beantwortet wurde.*
	☒ Ja, erfolgreiche und erfolglose		☐ Ja, nur erfolgreiche		
	☐ Ja, nur erfolglose		☐ Nein		

1.11	Wie lange werden diese Protokolldaten aufbewahrt? Geben Sie die Dauer in Tagen an. Tage	*Nur relevant, wenn 1.10 mit ja beantwortet wurde.*
1.12	Werden die Protokolle regelmäßig ausgewertet? ☐ Ja ☐ Nein ☒ Nein, eine Auswertung wäre aber im Bedarfsfall möglich	*Nur relevant, wenn 1.10 mit ja beantwortet wurde.*
1.13	Existiert ein mechanisches Schloss Büroräume?	☒ Ja ☐ Nein
1.14	Wird die Schlüsselausgabe protokolliert? Wenn ja, wer gibt die Schlüssel aus? Ausgabestelle: Bitte geben sie die Ausgabestelle an.	☐ Ja ☒ Nein
1.15	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? Wenn ja: Dienstanweisung, Besucher melden sich am Empfang und werden dort abgeholt und hinausbegleitet	☒ Ja ☐ Nein

2 Zutrittskontrollmaßnahmen zu Serverräumen						
2.1	Werden personenbezogene Daten des Auftraggebers auf Servern gespeichert, die von Ihnen oder etwaigen Dienstleistern betrieben werden?				☒ Ja ☐ Nein	
2.2	Standort des Serverraums / Rechenzentrums (RZ): KV Berlin Masurenallee 6A, 14057 Berlin KV Nordrhein, Tersteegenstraße 9, 40474 Düsseldorf				*Nur relevant, wenn 2.1 mit ja beantwortet wurde.*	
2.3	Sind die personenbezogenen Daten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)?				☐ Ja ☒ Nein	
2.4	Weitere Standorte: Geben Sie hier die in 2.3 betroffenen Standorte an.				*Nur relevant, wenn 2.3 mit ja beantwortet wurde.*	
2.5	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für alle im Einsatz befindlichen Server- / RZ Standorte? *Falls nein, beantworten Sie die folgenden Fragen bitte zusätzlich für alle weiteren Standorte separat.*				☒ Ja ☐ Nein	
2.6	Hat der Serverraum Fenster?				☐ Ja ☒ Nein	
2.7	Wie sind die Fenster vor Einbruch geschützt?				*Nur relevant, wenn 2.6 mit ja beantwortet wurde.*	
	☐ vergittert	☐ abschließbar	☐ alarmgesichert	☐ gar nicht	☐ Sonstiges	
	Bei Sonstiges geben Sie hier entsprechend weitere Informationen ein.					
2.8	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?				☒ Ja ☐ Nein	
2.9	Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!**				*Nur relevant, wenn 2.8 mit ja beantwortet wurde.*	
	☒ beauftragter Wachdienst	☐ Administrator		☒ Leiter IT	☐ Sonstiges	
	Bei Sonstiges geben Sie hier entsprechend weitere Informationen ein.					
2.10	Ist der Serverraum videoüberwacht?				☒ Ja, mit Aufzeichnung	

		☐ Ja, ohne Aufzeichnung ☐ Nein
2.11	Wie lange werden die Bilddaten gespeichert? 5 Tage	*Nur relevant, wenn 2.10 mit ja, mit Aufzeichnung beantwortet wurde.*
2.12	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: 10. Funktion im Unternehmen: IT-Systemadministratoren, IT-Abteilungsleitung, IT-Hauptabteilungsleitung, im Notfall Immobilienmanagement	
2.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? *Die Fragen 2.13 bis 2.17 sind nur relevant, wenn 2.12 mit ja beantwortet wurde.*	☒ Ja ☐ Nein
2.14	Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!**	
	☒ RFID / ☐ PIN / ☐ Biometrie / ☐ Sonstiges	
	Bei Sonstiges geben Sie hier entsprechend weitere Informationen ein.	
2.15	Werden die Zutrittsrechte personifiziert vergeben?	☒ Ja ☐ Nein
2.16	Werden die Zutritte zum Raum im Zutrittssystem protokolliert?	☒ Ja, erfolgreiche und erfolglose ☐ Ja, nur erfolgreiche ☐ Ja, nur erfolglose ☐ Nein
2.17	Wie lange werden die Zutrittsdaten gespeichert? 4 Wochen	
2.18	Wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus? Anzahl Schlüssel: Serverraum ist elektronisch gesichert, kein mechanisches Schloss Aufbewahrungsort: Tragen Sie den Aufbewahrungsort der Schlüssel ein. Ausgabestelle: Geben Sie an wo die Schlüssel ausgegeben werden.	
2.19	Aus welchem Material besteht die Zugangstür zum Serverraum?	☒ Stahl ☐ sonstiges Material
2.20	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt?	☒ Ja ☐ Nein
2.21	Was wird in dem Serverraum noch aufbewahrt?	*Nur relevant, wenn 2.20 mit ja beantwortet wurde.*
	☒ Telefonanlage / ☐ Lagerung Büromaterial / ☐ Lagerung Akten	
	☐ Archiv / ☐ Lagerung IT Ausstattung / ☐ Sonstiges	
	Bei Sonstiges geben Sie hier entsprechend weitere Informationen ein.	

3 Zugangs- und Zugriffskontrollmaßnahmen		
3.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen?	
	☒ Ja, es existiert ein definierter Freigabeprozess / ☐ Nein, die Vergabe erfolgt auf Zuruf	
	☐ Nein, die Vergabe erfolgt wie folgt: Bitte geben Sie an wie die Vergabe geregelt ist.	
3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert?	☒ Ja ☐ Nein
3.3	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst?	☒ Ja ☐ Nein
3.4	Existieren verbindliche Passwortparameter im Unternehmen?	☒ Ja ☐ Nein
3.5	Wie sind die Passwortparameter geregelt?	*Nur relevant, wenn 3.5 mit ja beantwortet wurde.*
	Passwort-Zeichenlänge: 10 (Muss: Groß-/Kleinbuchstaben und Ziffern) / Muss das Passwort Sonderzeichen enthalten? ☐ Ja ☒ Nein	
	Mindest-Gültigkeitsdauer: Bitte geben Sie die Dauer in Tagen an. Tage	
3.6	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben?	☒ Ja ☐ Nein
3.7	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? Wenn ja, nach wieviel Minuten? 10 Minuten	☒ Ja ☐ Nein
3.8	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts?	
	☐Keine / ☒Admin vergibt neues Initialpasswort	
	☐Sonstige Maßnahmen: Bitte nennen Sie die von Ihnen getroffenen Maßnahmen.	
3.9	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☐ Nein ☒ Ja, 3 maximal 5	
3.10	Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde?	*Nur relevant, wenn 3.9 mit ja beantwortet wurde.*
	☒ Bei 5 Fehlversuchen bleiben die Zugänge bis zur manuellen Aufhebung der Sperre gesperrt. / ☒ Bei 3 Fehlversuchen bleiben die Zugänge für 3 Minuten gesperrt.	
3.11	Wie erfolgt die Authentisierung bei Fernzugängen?	☒ Token ☒ VPN-Zertifikat ☒ Passwort
3.12	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☐ Nein ☒ Ja, 3 Fehlversuche, dann Sperrung	
3.13	Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche bei Fernzugriffen erreicht wurde?	*Nur relevant, wenn 3.12 mit ja beantwortet wurde.*
	☒ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt. / ☐ Die Zugänge bleiben für Bitte geben Sie die Sperrzeit in Minuten ein. Minuten gesperrt.	
3.14	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? Wenn ja, nach wieviel Minuten? Trennung nach max. 480 Minuten unabhängig von Aktivität/Inaktivität	☐ Ja ☒ Nein

3.15	Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert?		☒ Ja ☐ Nein
3.16	Wird die Firewall regelmäßig aktualisiert?		*Nur relevant, wenn 3.15 mit ja beantwortet wurde.*
	☒ Ja	☐ Nein	
3.17	Wer administriert Ihre Firewall?		*Nur relevant, wenn 3.15 mit ja beantwortet wurde.*
	☒ eigene IT	☒ externer Dienstleister	
3.19	Beim Einsatz eines externen Dienstleisters: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten?		*Nur relevant, wenn 3.18 mit ja beantwortet wurde.*
	☒ Ja	☐ Nein, die Aufschaltung ist nur mit Beteiligung eines Mitarbeiters der IT möglich.	

4 Maßnahmen zur Sicherung von Papierunterlagen, mobilen Datenträgern und mobilen Endgeräten			
4.1	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (z. B. Ausdrucke/Akten/Schriftwechsel) entsorgt?		
	☐ Altpapier / Restmüll	☒ Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist.	
	☒ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden.	☐ Sonstiges: Bitte geben Sie an wie die Entsorgung stattfindet.	
4.2	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt?		
	☐ Physische Zerstörung durch eigene IT	☒ Physische Zerstörung durch externen Dienstleister	
	☐ Löschen der Daten	☐ Löschen der Daten durch Bitte geben Sie die Anzahl an. Überschreibungen	
	☐ Sonstiges: Bitte geben Sie an wie die Entsorgung stattfindet.		
4.3	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks)?		☒ Ja ☐ Nein
4.4	Dürfen die Mitarbeiter private Datenträger (z.B. USB Sticks) verwenden?		
	☒ Nein	☐ Ja	
	☐ Ja, nach Genehmigung und Überprüfung		
4.5	Wie werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt?		
	☐ Verschlüsselung der Festplatte	☐ Verschlüsselung einzelner Verzeichnisse	
	☒ keine Verschlüsselung		
4.6	Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)?		☐ Ja ☒ Nein

5 Maßnahmen zur sicheren Datenübertragung			
5.1	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? Wenn ja, wie?		☒ Ja ☐ Nein
	☒ verschlüsselte Datei als Mailanhang	☐ verschlüsselter Datenträger	
	☐ per PGP / S / MIME	☒ https/TLS	

	☒ VPN	☒ SFTP	
	☐Sonstiges: Bitte geben Sie die Art der Verschlüsselung an.		
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate?		☐ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
5.3	Werden die Übertragungsvorgänge protokolliert?		☒ Ja ☐ Nein
5.4	Wie lange werden diese Protokolldaten (Empfangsbestätigungen) aufbewahrt? 10 Jahre		*Nur relevant, wenn 5.3 mit ja beantwortet wurde.*
5.5	Werden die Protokolle regelmäßig ausgewertet?		*Nur relevant, wenn 5.3 mit ja beantwortet wurde.*
	☐ Ja	☐ Nein	
	☒ Nein, eine Auswertung wäre aber im Bedarfsfall möglich.		

Maßnahmen zur Sicherstellung der Verfügbarkeit

1	**Serverraum**		
1.1	Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür?		☒ Ja ☐ Nein
1.2	Ist der Serverraum mit Rauchmeldern ausgestattet?		☒ Ja ☐ Nein
1.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen?		☒ Ja ☐ Nein
1.4	Ist der Serverraum mit Löschsystemen ausgestattet?		
	☐ Nein	☐ Ja, CO_2 Löscher	
	☒ Ja, Halon/Argon Löschanlage	☐ Ja, und zwar: Bitte geben Sie die Art des verwendeten Löschsystems an.	
1.5	Woraus bestehen die Außenwände des Serverraumes?		
	☒ Massivwand außen (z. B. Beton, Mauer)	☐ Leichtbauweise	
	☒ Brandschutzwand mit Feuerwiderstandsklasse ☐30 / ☐ 60 / ☒ 90		
1.6	Ist der Serverraum klimatisiert?		☒ Ja ☐ Nein
1.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung?		☒ Ja ☐ Nein
1.8	Wird die Stromversorgung des Serverraums zusätzlich über ein Dieselaggregat abgesichert?		☐ Ja ☒ Nein
1.9	Werden die oben genannten, vorhandenen Funktionalitäten (Rauchmelder, USW usw.) regelmäßig getestet?		☒ Ja ☐ Nein

2	**Backup- und Notfall-Konzept, Virenschutz**	
2.1	Gibt es ein Backupkonzept?	☒ Ja ☐ Nein
2.2	Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet?	☐ Ja ☒ ja, auf Datei-Ebene

		☐ Nein
2.3	In welchem Rhythmus werden Backups vom Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden?	
	☒ Echtzeitspiegelung / ☒ täglich	
	☒ ein- bis dreimal pro Woche / ☐ Sonstiges: Bitte geben Sie den verwendeten Rhythmus an.	
2.4	Auf was für Sicherungsmedien werden die Backups gespeichert?	
	☐Zwei redundante Server / ☒ Sicherungsbänder	
	☒ Festplatten / ☐ Sonstiges: Bitte geben Sie das verwendete Sicherungsmedium an.	
2.5	Wo werden die Backups aufbewahrt?	
	☐ Zweiter redundanter Server steht an einem anderen Ort / ☒ Safe (feuerfest, datenträger- und dokumentensicher)	
	☐ einfacher Safe / ☒ Bankschließfach	
	☒ Im Serverraum / ☐ abgeschlossener Aktenschrank / Schreibtisch	
	☐ Sonstiges: Bitte geben Sie den Aufbewahrungsort an.	
2.6	Im Falle eines Transports der Backups: Wie wird dieser durchgeführt?	
	☒ Transport durch einen MA der IT / ☐ Abholung durch Dritte (bspw. Bankmitarbeiter / Wachunternehmen)	
	☐ Sonstiges: Bitte Erläutern Sie kurz die Durchführung des Transports.	
2.7	Sind die Backups verschlüsselt?	☒ Ja ☐ Nein
2.8	Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil?	☒ Ja ☐ Nein
2.9	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement?	☒ Ja ☐ Ja, aber nicht dokumentiert ☐ Nein
2.10	Wer ist für das Software- bzw. Patchmanagement verantwortlich?	☐ Anwender selbst ☒ eigene IT ☒ externer Dienstleister
2.11	Gibt es ein Notfallkonzept (z. B. Notfallmaßnahmen bei Hardwaredefekten / Brand / Totalverlust etc.)?	☒ Ja ☐ Nein
2.12	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Wenn ja, durch: ☒aktuellem Virenschutz ☒aktueller Anti-Spyware ☒aktuellem Spamfilter	☒ Ja ☐ Nein
2.13	Wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich?	*Nur relevant, wenn 2.12 mit ja beantwortet wurde.*
	☐ Anwender selbst / ☒ eigene IT	
	☒ externer Dienstleister	

3 Netzanbindung

3.1	Verfügt das Unternehmen über eine redundante Internetanbindung?	☒ Ja ☐ Nein
3.2	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden?	☐ Ja ☐ Nein
3.3	Wer ist für die Netzanbindung des Unternehmens verantwortlich? ☒ eigene IT ☐ externer Dienstleister	

Pseudonymisierung / Verschlüsselung

1	**Einsatz von Pseudonymisierung**		
1.1	Werden verarbeitete personenbezogene Daten pseudonymisiert?		☐ Ja ☒ Nein
1.2	Werden Algorithmen zur Pseudonymisierung eingesetzt?		☐ Ja ☒ Nein
1.3	Welcher Algorithmus wird zur Pseudonymisierung eingesetzt? Bitte geben Sie den verwendeten Algorithmus an.		
1.4	Erfolgt eine Trennung der Zuordnungsdaten und eine Aufbewahrung in getrennten Systemen?		☐ Ja ☒ Nein
1.5	Wie kann die Pseudonymisierung bei Bedarf Rückgängig gemacht werden?		
	☐ gemäß einem definierten Verfahren	☐ im Mehr-Augen-Prinzip	
	☐ Auf Weisung des Vorgesetzten	☐ Sonstiges: Bitte erläutern Sie.	
2	**Einsatz von Verschlüsselung**		
2.1	Werden verarbeitete personenbezogene Daten über die bereits beschriebenen Maßnahmen hinaus verschlüsselt? Arztdaten, Patientendaten, Abrechnungsdaten		☒ Ja ☐ Nein
2.2	Welche Arten der Verschlüsselung werden eingesetzt?		
	☒ Ende-zu-Ende-Verschlüsselung	☒ Transportverschlüsselung	
	☐ Data-at-Rest-Verschlüsselung	☐ Andere Verschlüsselung: Bitte nennen Sie die verwendete Verschlüsselungsart.	
	Bitte nennen Sie für jede in 2.1 genannte Datenkategorie die entsprechend verwendete Verschlüsselungsart, sofern die Verschlüsselung sich unterscheidet. Für alle unter 2.1 genannten Datenkategorien wird eine symmetrische und asymmetrische Verschlüsselung eingesetzt		
2.3	Welche kryptographischen Algorithmen werden zur Verschlüsselung oder für verschlüsselungsartige Maßnahmen (z. B. Hashen von Passwörtern) eingesetzt?		
	☒ AES	☒ SHA-256	
	☐ RSA-2048	☐ Sonstige: Bitte nennen Sie die verwendeten Algorithmen.	
2.4	Wer hat Zugriff auf die Verschlüsselten Daten? Mitarbeiter aus den Abteilungen: Fachabteilungen (IT und Honorarabrechnung) Insgesamt haben ca. 15 Mitarbeiter Zugriff auf verschlüsselte Daten.		

Sonstige Maßnahmen nach Art. 32 Abs. 1 lit. b,c,d DSGVO

1	**Belastbarkeit**	
	Es existieren Maßnahmen, die die Fähigkeit gewährleiten, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Regelmäßige Penetrationtests	☒ Ja ☐ Nein
2	**Wiederherstellbarkeit**	
	Existieren Notfall- oder Recovery-Konzepte und Maßnahmen über B.2.11 hinaus, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen? Bitte Beschreiben Sie die Maßnahmen.	☐ Ja ☒ Nein
3	**Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen**	
3.1	Existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung? Regelmäßige Penetrationtests	☒ Ja ☐ Nein
3.2	In welchen Abständen finden die Überprüfungen statt? Mindestens jährlich	
3.3	Werden die Ergebnisse der Prüfungen dokumentiert?	☒ Ja ☐ Nein
3.4	Gibt es Zertifizierungen mit Bezug zu den technisch-organisatorischen Maßnahmen? Wenn ja, welche? Bitte nennen Sie vorhandene Zertifizierungen.	☐ Ja ☒ Nein