



Auftragsverarbeitungsvertrag

mit Anlage der technischen und organisatorischen Maßnahmen, gemäß Art. 28 DS-GVO
zwischen dem **Auftraggeber** und dem **Auftragsverarbeiter, der ARNI**.

Erläuterung zum Auftragsverarbeitungsvertrag

Bei diesem Auftragsverarbeitungsvertrag (AV-Vertrag) geht es um die Sicherheit der personenbezogenen Daten, die Sie als Behandler oder Leistungserbringer im Gesundheitswesen, uns als Ihrem Abrechnungsdienstleister übermitteln.

Ihre Patienten, Kunden und Mitarbeiter haben einen Vertrag mit Ihnen bzw. Ihrem Unternehmen und nicht mit uns als Ihrem Abrechnungsdienstleister. Daher ist der Abschluss vorstehenden Auftragsverarbeitungsvertrages zwischen Ihnen bzw. Ihrem Unternehmen und uns notwendig, damit zwischen Ihnen bzw. Ihrem Unternehmen und uns geregelt ist, wie wir mit den uns zu Abrechnungszwecken zur Verfügung gestellten personenbezogenen Daten umzugehen haben. Auf diese Weise können Sie auch Ihren Patienten, Kunden und Mitarbeitern gegenüber gewährleisten, dass deren Daten bei uns so behandelt werden, wie es von den Patienten, Kunden und Mitarbeitern mit Ihnen bzw. Ihrem Unternehmen vereinbart wurde.

§ 1 Auftragsgegenstand

Der Auftragsverarbeiter wird im Auftrag des Auftraggebers auf der Grundlage des zwischen den Vertragsparteien abgeschlossenen Geschäftsbesorgungsvertrages über Abrechnungsleistungen als Rechenzentrum/Abrechnungsstelle i.S.d. § 302 Abs. 2 SGB V (bzw. § 105 SGB XI für Pflegeleistungen) tätig. Im Rahmen des Auftrags werden personenbezogene Daten gemäß Art. 4 Abs. 1 DSGVO, Gesundheitsdaten gemäß Art. 9 Abs. 1 DSGVO sowie Sozialdaten gemäß SGB X (im Folgenden kurz: „personenbezogene Daten“), die aus dem Verfügungsbereich des Auftraggebers stammen, von diesem an den Auftragsverarbeiter übergeben, der die personenbezogenen Daten zu Abrechnungszwecken verarbeitet. Es liegt in der ausschließlichen Verantwortung des Auftraggebers, die Art, den Umfang und den Zweck der Verarbeitung der Daten des Auftraggebers zu bestimmen.

Der vorliegende Vertrag zur Auftragsverarbeitung beinhaltet die Übermittlung und Verarbeitung folgender personenbezogener Daten, Gesundheitsdaten und Sozialdaten:

- (1) Stammdaten der Versicherten/Patienten (Name, Anschrift, Geburtsdatum)
- (2) Krankenversicherungsdaten (Versichertennummer, Kostenträger/Krankenkasse, Versichertenstatus)
- (3) Gesundheits- und Sozialdaten (Diagnosen soweit für die Abrechnung erforderlich, verordnete Heil-/Hilfsmittel, Behandlungsdaten) – besondere Kategorien nach Art. 9 DS-GVO
- (4) Verordnungs-/Rezeptdaten (verordnende Ärztin/Arzt, Ausstellungs-/Verordnungsdatum)
- (5) Abrechnungs- und Leistungsdaten (erbrachte Leistungen, Mengen, Beträge, Abrechnungszeitraum)
- (6) Zahlungs- und Bankdaten von Privatpatienten (für Rechnungsstellung/Forderungseinzug)

Folgende Kategorien betroffener Personen sind von der Verarbeitung erfasst (Art. 28 Abs. 3 Satz 1 DS-GVO):

- Versicherte und Patientinnen/Patienten des Auftraggebers (gesetzlich Versicherte sowie Privatpatienten und Selbstzahler)
- verordnende Ärztinnen und Ärzte
- Angehörige, gesetzliche Vertreter, amtlich bestellte Betreuer bzw. sonstige Rechnungsempfänger, soweit in den Unterlagen enthalten
- Beschäftigte des Auftraggebers, soweit deren Daten in Abrechnungsunterlagen enthalten sind (z.B. Beschäftigtennummer nach § 302 Abs. 1 Satz 2 SGB V)

Folgende Dienstleistungen werden erbracht:

- (1) Rezeptabrechnung – Digitalisierung, Erfassung, Prüfung und Abrechnung der eingereichten Verordnungen gegenüber Krankenkassen und gesetzlichen Kostenträgern (§ 302, § 127 SGB V)
- (2) Rechnungsstellung und Mahnwesen gegenüber Privatpatienten/Selbstzahlern
- (3) Übernahme des Schriftverkehrs/der Korrespondenz mit den Kostenträgern

Hinsichtlich des Beginns, der Dauer und der Beendigung dieses Vertrages gelten die Regelungen des zwischen den Parteien geschlossenen Geschäftsbesorgungsvertrages über Abrechnungsdienstleistungen.

§ 2 Weisungsgebundenheit

Der Auftragsverarbeiter ist bei der Auftrags Erfüllung zur Verarbeitung personenbezogener Daten nur im Rahmen der Weisungen des Auftraggebers berechtigt. Diese Weisungen bedürfen mindestens der Textform.

Jede Übermittlung personenbezogener Daten in ein Drittland darf nur nach vorheriger Weisung des Auftraggebers und nur unter Einhaltung der Voraussetzungen von Art. 44-50 DSGVO erfolgen (z.B. EU – Standardvertragsklauseln).

§ 3 Meldepflicht

Der Auftragsverarbeiter hat dem Auftraggeber unverzüglich, spätestens binnen 24 Stunden, nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten (Datenpanne) im Sinne von Art. 33 DSGVO Meldung zu machen. Die Meldung hat in Textform zu erfolgen. Im Rahmen der Meldung hat der Auftragsverarbeiter dem Auftraggeber die in Art. 33 Abs. 3 DSGVO im Einzelnen aufgelisteten Informationen zur Verfügung zu stellen.

Der Auftragsverarbeiter hat den Auftraggeber unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen die europäische Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG), den Sozialdatenschutz oder berufliche Verschwiegenheitsverpflichtungen (§ 203 StGB) oder andere, insbesondere spezialgesetzliche Vorschriften über den Datenschutz verstößt.

Auftragsverarbeiter und Auftraggeber werden sich gegenseitig unverzüglich informieren, wenn Störungen, Unregelmäßigkeiten oder der Verdacht auf Datenschutzverletzungen auftreten. Insbesondere wird der Auftragsverarbeiter den Auftraggeber unverzüglich

ARNI - Abrechnungsstelle Niedersachsen für Heil- und Hilfsmittel GmbH

Auftragsverarbeitungsvertrag, Stand: 01.07.2026 – Seite 3

schriftlich unterrichten, wenn die Datenschutzbehörden (Landesbeauftragte für Datenschutz und Informationsfreiheit) Mängel im Betrieb des Auftragsverarbeiters feststellen, die auch die Datenverarbeitung für den Auftraggeber betreffen.

§ 4 Verpflichtung auf das Datengeheimnis und die Schweigepflicht (§ 203 StGB)

Der Auftragsverarbeiter ist verpflichtet, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten für den Auftraggeber die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 sowie Art. 29, 32 Abs. 4 DS-GVO zu gewährleisten. 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter 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.

Soweit der Auftraggeber einem Berufsgeheimnis nach § 203 StGB unterliegt, wird der Auftragsverarbeiter als mitwirkende Person im Sinne des § 203 Abs. 3 Satz 2 StGB tätig. Der Auftragsverarbeiter verpflichtet sich zur Geheimhaltung aller ihm im Rahmen der Auftragsdurchführung bekanntwerdenden fremden Geheimnisse, insbesondere Patientengeheimnisse. Er wird sämtliche bei der Auftragsdurchführung eingesetzten Personen vor Aufnahme ihrer Tätigkeit gemäß § 203 Abs. 4 StGB zur Geheimhaltung verpflichten, sie über die Strafbarkeit einer unbefugten Offenbarung belehren und dies dokumentieren; die Verpflichtung ist dem Auftraggeber auf Verlangen nachzuweisen. Werden Unterauftragnehmer eingesetzt, hat der Auftragsverarbeiter diesen die gleichen Geheimhaltungspflichten aufzuerlegen.

§ 5 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 (sofern sie eine Nebenleistung sind), die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung in Anspruch nimmt. Der Auftragsverarbeiter 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 Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Dazu hat der Auftragsverarbeiter den Auftraggeber 4 Wochen vor der geplanten Nutzung eines Unterauftragnehmers dies anzukündigen. Der Auftraggeber verpflichtet sich, innerhalb von 2 Wochen nach Eingang der Ankündigung darauf schriftlich zu reagieren. Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer [siehe Anlage 2] zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS- GVO.
- (3) Bei der Unterbeauftragung sind dem Unterauftragnehmer die gleichen vertraglichen Regelungen aufzuerlegen, wie sie für den Auftragsverarbeiter gelten. Dem Auftraggeber sind gegenüber dem Unterauftragnehmer die gleichen Weisungs-, Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und dem Art. 28 DSGVO einzuräumen, wie sie gegenüber dem Auftragsverarbeiter gelten.
- (4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 6 Mitwirkungs- und Unterstützungspflichten

Der Auftragsverarbeiter verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. e und f DSGVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen (insb. bei Auskunfts-, Berichtigungs- und Löschungsanträgen von Betroffenen) zu unterstützen.

Für vorstehende Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragsverarbeiter eine angemessene Vergütung verlangen.

§ 7 Datenschutzbeauftragter

Als Datenschutzbeauftragter ist beim Auftragsverarbeiter benannt:

Jürgen Recha, c/o interev GmbH, Robert-Koch-Straße 55, 30853 Langenhagen, 0511 89798410, info@interrev.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragsverarbeiters leicht zugänglich hinterlegt. Stellt der Datenschutzbeauftragte in diesem Zusammenhang Unregelmäßigkeiten fest, ist unverzüglich der Datenschutzbeauftragte des Auftraggebers oder ein sonstiger, für Datenschutzangelegenheiten benannter Mitarbeiter des Auftraggebers, zu informieren.

§ 8 Rechte der Betroffenen, Datenschutzfolgeabschätzung

Die Rechte, die durch die Datenverarbeitung beim Auftragsverarbeiter betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Er ist verantwortlich für die Wahrung dieser Rechte. Der Auftragsverarbeiter hat den Auftraggeber bei der Wahrung dieser Rechte, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung im Rahmen seiner Möglichkeiten zu unterstützen.

Wenn Anfragen von Betroffenen beim Auftragsverarbeiter eingehen, dann leitet dieser die Anfragen unverzüglich an den Auftraggeber weiter.

ARNI - Abrechnungsstelle Niedersachsen für Heil- und Hilfsmittel GmbH

Auftragsverarbeitungsvertrag, Stand: 01.07.2026 – Seite 4

Im Falle des Vorliegens der Voraussetzungen des Art. 35 Abs. 1 DS-GVO wird der Auftragsverarbeiter den Auftraggeber bei der erforderlichen Datenschutzfolgeabschätzung nach Maßgabe der Regelungen in Art. 35 Abs. 7 DS-GVO unterstützen.

§ 9 Datentransport, Datenberichtigung sowie -sperre

Die Verantwortung für den Transport der Daten obliegt dem Auftraggeber. Der Transport elektronischer Daten zwischen Auftraggeber und Auftragsverarbeiter erfolgt mittels geeigneter Verschlüsselungsverfahren. Der Auftragsverarbeiter weist dem Auftraggeber die von ihm üblicherweise eingerichteten Verlustsicherungsmaßnahmen nach. Zusätzliche Anforderungen des Auftraggebers und daraus resultierende Maßnahmen sind schriftlich zu vereinbaren.

Der Auftragsverarbeiter wird Weisungen des Auftraggebers im Zusammenhang mit der Berichtigung, Löschung oder der Sperre von überlassenen Daten der Kunden des Auftraggebers unverzüglich umsetzen.

§ 10 Nachvertragliche Pflichten, Datenlöschung

Bei Beendigung des Auftragsverhältnisses verpflichtet sich der Auftragsverarbeiter, alle ihm aus Anlass und im Zusammenhang mit der Auftragsabwicklung übergebenen Unterlagen nach Wahl des Auftraggebers zeitgerecht (innerhalb von 4 Wochen) zurückzugewähren bzw. den Nachweis der ordnungsmäßigen Vernichtung zu führen, soweit der Auftragsverarbeiter nicht aufgrund gesetzlicher Vorschriften zur längeren Aufbewahrung verpflichtet ist.

Von der Vernichtung innerhalb vorstehend geregelter Fristen sind ebenfalls ausgenommen diejenigen Daten, die der Auftragsverarbeiter gemäß Ziffer 28 Abs.2 des Geschäftsbesorgungsvertrages noch bis zu 60 Tagen nach Beendigung des Geschäftsbesorgungsvertrages zu seiner Sicherheit benötigt. Die hier geregelten Pflichten gelten für diese Daten erst nach Ablauf der 60 Tage und sind erst dann innerhalb vorstehend geregelter Fristen an den Auftraggeber zurückzugewähren bzw. ist gegenüber dem Auftraggeber innerhalb dieser Fristen der Nachweis der ordnungsmäßigen Vernichtung zu führen.

Dokumentationen, die dem Nachweis der ordnungsmäßigen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren, sofern die Verpflichtung zur Aufbewahrung nicht durch den Auftraggeber übernommen wird.

Der Auftragsverarbeiter hat im Regressfall dem Auftraggeber auch nach Vertragsende etwaig noch vorhandene Dokumentationen zur Führung des Entlastungsbeweises zu überlassen. Eine entsprechende Pflicht zur Datenlöschung trifft den Auftragsverarbeiter, sofern der Auftraggeber den Auftragsverarbeiter entsprechend schriftlich anweist.

Die Vertragsparteien sind verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus Stillschweigen über die im Zusammenhang mit dem Auftrag bekannt gewordenen Daten zu wahren.

§ 11 Technische und organisatorische Datenschutzmaßnahmen

Der Auftragsverarbeiter 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 durch ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, und Art. 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.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 12 Zweckbindung der Daten

Der Auftragsverarbeiter verarbeitet die überlassenen Daten ausschließlich zu den vertraglich vereinbarten Zwecken (Rezeptabrechnung, Rechnungsstellung, Mahnwesen, Korrespondenz mit dem Auftraggeber und Kostenträgern und sonstigen Forderungsschuldnern). Als Rechenzentrum i.S.d. § 302 Abs. 2 SGB V verarbeitet er die ihm zur Abrechnung übermittelten Daten nur für im Sozialgesetzbuch bestimmte Zwecke und nur in einer auf diese Zwecke ausgerichteten Weise (§ 302 Abs. 2 S. 3 SGB V). Eine Verarbeitung zu anderen Zwecken oder eine Weitergabe an Dritte ist unzulässig; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet werden. Gesetzliche Übermittlungspflichten (z.B. § 302 Abs. 2 S. 4 und 5 SGB V an Kassenärztliche Vereinigungen) bleiben unberührt.

§ 13 Kontrollmaßnahmen des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Bestimmungen sowie der Verpflichtungen aus diesem Vertrag im Unternehmen des Auftragsverarbeiters vor Beginn der Datenverarbeitung und sodann einmal jährlich bzw. aus gegebenem Anlass zu überprüfen. Zu diesem Zwecke wird der Auftragsverarbeiter dem Auftraggeber bzw. von diesen beauftragten Mitarbeitern oder sonstigen Dritten Zugang zu den Geschäftsräumen, in denen Datenverarbeitungsprozesse für den Auftraggeber stattfinden bzw. stattfinden sollen, sowie Zugriff auf erforderliche Unterlagen und/oder Daten gewähren. Ferner wird der Auftragsverarbeiter sämtliche Mitwirkungspflichten erbringen, die für eine effiziente Kontrolle der Einhaltung der datenschutzrechtlichen Pflichten des Auftragsverarbeiters durch den Auftraggeber erforderlich sind.

Der Auftragsverarbeiter ist darüber unterrichtet, dass der Auftraggeber die Ergebnisse seiner Kontrollen dokumentiert. Der Auftraggeber wird dem Auftragsverarbeiter auf dessen schriftliches Verlangen Auskunft über das Ergebnis seiner Kontrollen erteilen.

§ 14 Gerichtsstand

Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist Hannover.

ARNI - Abrechnungsstelle Niedersachsen für Heil- und Hilfsmittel GmbH

Auftragsverarbeitungsvertrag, Stand: 01.07.2026 – Seite 5

§ 15 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung des Schriftformerfordernisses selbst.

Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen Bestimmung tritt die entsprechende gesetzliche Regelung. Gleiches gilt für den Fall, dass eine Regelung undurchführbar wird oder diese Vereinbarung eine Regelungslücke enthält.

Anlage 1: Technische und organisatorische Maßnahmen, gem. Art. 32 Abs. 1 DS-GVO

1. Verschlüsselung

Eine Verschlüsselung erfolgt in Abhängigkeit der Daten, des Auftrags sowie der Umsetzungsmöglichkeit. Die Verschlüsselung erfolgt mit angemessener Verschlüsselungstechnik in Abhängigkeit zu den technischen, organisatorischen und finanziellen Mitteln.

Eine Verschlüsselung der Datentransfers ist bei dem vorliegenden Vertrag vereinbart.

2. Gewährleistung der Vertraulichkeit

Zutrittskontrolle:

Übersicht aller getroffenen Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, zu verwehren.

- ☒Sorgfältige Auswahl von Reinigungspersonal
- ☒Personenkontrolle beim Empfang, Chipkarten-/Transponder-Schließsystem
- ☒Schließsystem mit Chipsperre
- ☒Manuelles Schließsystem
- ☒Schlüsselregelung (Schlüsselausgabe etc.)
- ☒Sicherheitsschlösser
- ☒Protokollierung der Besucher

Zugriffskontrolle:

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten 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 der Vernichtung
- ☒Sichere Aufbewahrung von Datenträgern
- ☒ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☒Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒Verschlüsselung von Datenträgern
- ☒Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Belehrung der Mitarbeiter:

- ☒Schulung durch Datenschutzbeauftragten
- ☒Schulungen von lawpilots zu Informationssicherheit, Datenschutz und Compliance

Trennungskontrolle:

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

- ☒physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒Erstellung eines Berechtigungskonzepts
- ☒Trennung von Produktiv- und Testsystem
- ☒Festlegung von Datenbankrechten
- ☒Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System (Testsystem vs. Produktivsystem)
- ☒Versehen der Datensätze mit Zweckattributen/Datenfeldern

3. Gewährleistung der Integrität

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.

ARNI - Abrechnungsstelle Niedersachsen für Heil- und Hilfsmittel GmbH

Auftragsverarbeitungsvertrag, Stand: 01.07.2026 – Seite 6

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ 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

4. Gewährleistung der Verfügbarkeit

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 in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Testen von Datenwiederherstellung
- ☒ Erstellen eines Notfallplans
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Serverräume nicht unter sanitären Anlagen
- ☒ Datensicherung täglich
- ☒ Virenschutzkonzept
- ☒ Notfallplan

5. Gewährleistung der Belastbarkeit der Systeme

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

- ☒ Storage-Systeme nach Stand der Technik (bzgl. Toleranz und Resilienz ggü. Fehlern und Störungen)
- ☒ Backup Hard- und Software sind nach Stand der Technik ausgewählt und eingesetzt
- ☒ Notfallkonzepte
- ☒ Kapazitätsmanagement
- ☒ Patch-Management
- ☒ tägliche Datensicherung

6. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- ☒ Notfallplan
- ☒ Kontinuitätsmanagement - Konzept Spiegelungen in Externe Rechenzentren
- ☒ Redundante Datenspeicherung
- ☒ Regelmäßige Tests der Backups auf Datenwiederherstellung
- ☒ Backup- und Recoverykonzept

7. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Maßnahmen, die gewährleisten, dass eine systematische und regelmäßige Überprüfung sowie eine sach- und fachgerechte Bewertung und Behandlung der Wirksamkeit der technischen und organisatorischen Maßnahmen erfolgt.

- ☒ Datenschutzmanagement installiert regelmäßige Tests/Risikoanalyse inkl. Dokumentation (für den Bereich IT)
- ☒ Interne Audits, Externe Audits
- ☒ Kontrolle durch externen Datenschutzbeauftragten

Anlage 2: Unterauftragnehmer

Unterauftragnehmer	Anschrift	Leistung	Abgesichert durch (AV-Vertrag, SCC, TIA, Garantien)
CTR Hannover, Hr. Jan Reimers	Garbsener Landstr. 10, 30419 Hannover	IT Dienstleister	AV-Vertrag