

## Vereinbarung

zwischen dem

Medizinischen Dienst RLP, Albiger Str. 19 d, 55232 Alzey  
.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

.....  
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt  
.....]

### 1. Gegenstand und Dauer des Auftrags

#### (1) Gegenstand

✗ Der Gegenstand des Auftrags ergibt sich aus der  
Leistungsvereinbarung/SLA/.....RLP260121Intranet..... vom 18.06.2026, auf die hier  
verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch  
den Auftragnehmer: ..... (Definition der Aufgaben)

#### (2) Dauer

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

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von .....  
zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon  
unberührt.

 <b>Medizinischer Dienst Rheinland-Pfalz</b>	<b>Vertrag zur Auftragsverarbeitung im Medizinischen Dienst Rheinland-Pfalz</b>	Seite: 2/14 Stand: 03/2026
---	---	-------------------------------

## 2. Konkretisierung des Auftragsinhalts

### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

- ✗ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom ~~18.06.2026~~

oder

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

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede Verlagerung in ein Land außerhalb des Geltungsbereiches der DSGVO ist unzulässig.

### (2) Art der Daten

- ✗ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Sozialdaten
- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ ...

### (3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

- ✗ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Versicherte /Angehörige
- ☐ Leistungserbringer
- ☒ Auftraggeber
- ☒ Beschäftigte des Auftraggebers

- ☐ Externe Gutachterinnen/Externe Gutachter
- ☐ Mitglieder Verwaltungsrat
- ☐ Vertreterinnen/Vertreter im Beirat
- ☒ Personalrat
- ☒ Sonstige: externe Personen (z.B. Betriebsärztin)

### 3. Technisch-organisatorische Maßnahmen

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

### 4. Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- b) ☒ Der Auftragnehmer ist **nicht** zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau

.....  
[Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

- c) Der Auftragnehmer ermöglicht und unterstützt Kontrolltätigkeiten des Datenschutzbeauftragten des Medizinischen Dienstes sowie des Landesdatenschutzbeauftragten.
- d) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 c, 32 DS-GVO sind zu gewährleisten [Einzelheiten in Anlage 1].
- f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, ist zu gewährleisten. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der

Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- j) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages, ist zu gewährleisten.

## 6. Unterauftragsverhältnisse

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Hierzu gehören auch Aufträge für die Hard- und Software-Wartung, Benutzerservice, die Entsorgung von Datenträgern als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen, bei denen die Möglichkeit besteht, dass personenbezogene Daten/Sozialdaten (n. Art. 9 DSGVO) des Auftraggebers (Verantwortlichen) zur Kenntnis genommen werden könnten.
- (2) Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers (Verantwortlichen) auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (3) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
  - a) ☒ Eine Unterbeauftragung ist unzulässig.
  - b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

- c) ☐ Die Auslagerung auf Unterauftragnehmer oder
  - ☐ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:
    - der Auftraggeber (Verantwortliche) ab Zugang der Anzeige durch den Auftragnehmer innerhalb von 3 Monaten der Auslagerung auf /dem Wechsel des Unterauftragnehmers schriftlich oder in Textform zugestimmt hat (oder: zustimmt)

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Der Anzeige an den Auftraggeber (Verantwortlichen) sind

- der mit dem Unterauftragnehmer ausverhandelte Hauptvertrag,
  - die ausverhandelte Vereinbarung zur Auftragsvereinbarung sowie
  - die vorausgefüllte Anzeige nach § 80 SGB X
- beizufügen.

**Hinweis: Der Hauptvertrag und die AV-Vereinbarung mit dem Unterauftragnehmer dürfen noch nicht abgeschlossen sein.**

- (4) Die Weitergabe von personenbezogenen Daten des Auftraggebers (Verantwortlichen) an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (5) Eine weitere Auslagerung durch den Unterauftragnehmer  
ist nicht gestattet;  
bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);  
bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);  
sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.
- (6) Die Beauftragung von Unterauftragnehmern außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung ist unzulässig.

## 7. Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.
- (3) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

- (4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- ✗ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
  - ✗ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
  - ✗ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, Datenschutzauditoren);
  - ✗ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
- (5) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (6) Der Auftragnehmer hat sicherzustellen, dass der Auftraggeber (Verantwortliche) gegenüber jedem Unterauftragnehmer bzw. dessen weitere Unterauftragnehmer seine Kontrollrechte aus dieser Vereinbarung unmittelbar selbst ausüben kann. Das Kontrollrecht steht auch dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz zu.

## 8. Mitteilung bei Verstößen des Auftragnehmers

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

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

## 9. Weisungsbefugnis des Auftraggebers

- (1) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.
- (2) Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.



- (3) **Opt.** Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind: z. B. Vorstand, IT-Leitung, Projektleitung usw.
- (4) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

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

## 11. Optional Fernzugriff bei Prüfung/Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

- (1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.
- (2) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.
- (3) Die Mitarbeiterinnen und Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.



- (4) Vor Durchführung von Fernzugriffen werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.
- (5) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
- (6) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.
- (7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisaufnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.
- (8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Bei Datenabzug der Wirkdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.
- (9) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen, wie im Anhang beschrieben, ergreifen.
- (10) Die oben genannten Punkte gelten auch für Unterauftragnehmer, wenn diese gemäß Punkt 6 „Unterauftragsverhältnisse“ Absatz 2 erlaubt sind.

## 12. Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

## 13. Haftung

- (1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

- (2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
- a. er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
  - b. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
  - c. er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.
- (3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.
- (4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
- a. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
  - b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.
- (5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

#### 14. Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

#### 15. Salvatorische Klausel

- (1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
- (2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
- (3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.
- (4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter -Ziffer 15 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

 <b>Medizinischer Dienst Rheinland-Pfalz</b>	<b>Vertrag zur Auftragsverarbeitung im Medizinischen Dienst Rheinland-Pfalz</b>	Seite: 11/14 Stand: 03/2026
---	---	--------------------------------

## 16. Rechtswahl, Gerichtsstand

- (1) Es gilt deutsches Recht.
- (2) Gerichtsstand ist der Sitz des Auftraggebers.

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift Auftraggeber

\_\_\_\_\_  
Unterschrift Auftragnehmer

## Anlage 1– Technisch-organisatorische Maßnahmen

### 1. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 a DS-GVO)

- Pseudonymisierung (Art. 32 Abs. 1 a DS-GVO; Art. 25 Abs. 1 DS-GVO) ist die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.
- Verschlüsselung bedeutet unter Berücksichtigung des Stands der Technik ein angemessenes Schutzniveau zu erreichen.

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

- Zutrittskontrolle  
Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen; zu verwehren.
- Zugangskontrolle  
Unbefugten ist die Systembenutzung, z.B. durch: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung unter Berücksichtigung des Stands der Technik; zu verwehren.
- Zugriffskontrolle  
Es ist zu gewährleisten, dass ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen; verhindert wird.
- Trennungskontrolle  
Es ist die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing; zu gewährleisten.

### 3. Integrität (Art. 32 Abs. 1 b DS-GVO)

- Weitergabekontrolle  
Es ist zu gewährleisten, dass ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur; verhindert wird.
- Eingabekontrolle  
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement; ist zu gewährleisten.

#### 4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 c DS-GVO)

- Verfügbarkeitskontrolle  
Der Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne); ist zu gewährleisten.
- Eine rasche Wiederherstellbarkeit ist zu gewährleisten.

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle  
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

 Medizinischer Dienst Rheinland-Pfalz	<b>Vertrag zur Auftragsverarbeitung im  Medizinischen Dienst Rheinland-Pfalz</b>	Seite: 14/14 Stand: 03/2026
--	--	--------------------------------

# Anlage 2 zum AV-Vertrag: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung