AUFTRAGSVERARBEITUNGSVERTRAG (AV-VERTRAG)

gemäß Artikel 28 EU-DS-GVO

zwischen

Max-Delbrück-Centrum für Molekulare Medizin in der Helmholtz-Gemeinschaft
vertreten durch den Vorstand
Robert-Rössle-Str. 10, 13125 Berlin, Deutschland

– im Folgenden: **MDC** genannt –

und

dem

[- Auftragsverarbeiter – nachstehend Auftragnehmer genannt**]**

vertreten durch

,

– im Folgenden: **Auftragnehmer** genannt –

...

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung / SLA / *[Art des Rahmenvertrags]* vom *[Datum]*, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: *[Nennung 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 *[Datum].*

(3) Wartung

Soweit der Auftragnehmer für den Auftraggeber Wartungsarbeiten an IT-Systemen durchführt, gelten zusätzlich folgende Vereinbarungen:

Der Auftragnehmer darf im Rahmen der Wartung nur auf personenbezogene Daten des Auftraggebers zugreifen, wenn dies für die Durchführung der Wartung erforderlich ist. Es ist dem Auftragnehmer bei der Wartung untersagt, personenbezogene Daten des Auftraggebers auf eigenen IT-Systemen oder Datenträgern zu speichern, es sei denn, der Auftraggeber weist ihn hierzu an.

Fernwartungsarbeiten hat der Auftragnehmer dem Auftraggeber im Vorfeld anzukündigen. Der Auftraggeber ist berechtigt, die Durchführung der Fernwartung mitzuverfolgen. Der Auftragnehmer hat sicherzustellen, dass alle Wartungsvorgänge kontrolliert und nachvollzogen werden können. Auf Anfrage und soweit erforderlich, wirkt der Auftragnehmer an der Konfiguration technischer Kontrolleinrichtungen mit.

Die Fernwartung ist nur von Geschäftsräumen des Auftragnehmers aus zulässig. Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen. Der Auftragnehmer verwendet nach dem Stand der Technik hinreichend sichere Authentisierungsverfahren.

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung der Daten

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

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: *[Beschreibung]*

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 Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Textform und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in *[Nennung des Landes]* ...

☐ ... ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DSGVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. Art. 40 DSGVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DSGVO);

☐ wird hergestellt durch sonstige Maßnahmen: *[Nennung]* (Art. 46. Abs. 2 lit. a, Abs. 3 lit. a und b DSGVO)

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: *[Nennung]*

oder

☐ Gegenstand der Vereinbarung personenbezogener Daten sind folgende Datenarten/-kategorien:

- ☐ Personenstammdaten/Kontaktdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail; IP-Adresse)
- ☐ Vertrags-, -anbahnungs- und -abrechnungsdaten, Buchungs- und Zahldaten
- ☐ Pseudonyme
- ☐ Planungs- und Steuerungsdaten
- ☐ Daten aus denen die Leistung/Bewertung von Personen hervorgehen kann
- ☐ besondere Kategorien personenbezogener Daten:
- ☐ Daten über die Gesundheit
- ☐ Daten aus Fragebögen
- ☐ Daten aus Testungen
- ☐ genetische Daten
- ☐ biometrische Daten
- ☐ Biomaterialproben
- ☐ Bilddaten
- ☐ Audiodaten über Ton-/ Stimmenaufnahmen
- ☐ Videodaten über Ton- und Bildaufnahmen
- ☐ Daten über das Sexualleben
- ☐ Daten über die sexuelle Orientierung
- ☐ Daten über die rassische oder ethnische Herkunft
- ☐ Daten über die religiöse Überzeugung
- ☐ Daten über die weltanschauliche Überzeugung
- ☐ Daten über die politische Meinung
- ☐ Daten über die Gewerkschaftszugehörigkeit

☐ andere: *[Nennung]*

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: *[Nennung]*

oder

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Beschäftigte des Auftraggebers
- ☐ Beschäftigte eines Dritten
- ☐ Interessenten
- ☐ Probanden des Auftraggebers
- ☐ Lieferanten
- ☐ Ansprechpartner
- ☐ andere: *[Nennung]*

§ 3 Technische und 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 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen und während der Dauer der Verarbeitung personenbezogener Daten des Auftraggebers aufrechtzuerhalten. 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 2].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet,

nach vorheriger Zustimmung des Auftraggebers in Textform, alternative adäquate technische und organisatorische Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der bereits in Anlage 2 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, spätestens aber innerhalb von 3 Tagen, an den Auftraggeber weiterleiten und ohne entsprechende Einzelanweisung des Auftraggebers nicht mit der betroffenen Person in Kontakt treten.

(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 trägt zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gem. Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gem. Art. 38 und 39 DSGVO 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 bestellt:

[Vorname, Name, Organisationseinheit, Telefon, E-Mail].

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers einfach zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird benannt:

[Vorname, Name, Organisationseinheit, Telefon, E-Mail] .

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Europäischen Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union:

[Vorname, Name, Organisationseinheit, Telefon, E-Mail] .

d) Die Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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 gem. Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 2].

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

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

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

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

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

k) Der Auftragnehmer erkennt insbesondere an, dass er für die Auftragsverarbeitung das Berliner Datenschutzgesetz einzuhalten hat und unterwirft sich insofern der Kontrolle der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

§ 6 Unterauftragsverhältnisse

(1) Der Auftragnehmer darf weitere Auftragsverarbeiter hinsichtlich der Verarbeitung personenbezogener Daten des Auftraggebers nur nach vorheriger Zustimmung des Auftraggebers in Textform hinzuziehen. Dies gilt in gleicher Weise für den Fall, dass weitere Unterauftragsverhältnisse durch weitere Auftragsverarbeiter begründet werden. Der Auftragnehmer stellt sicher, dass eine entsprechende Zustimmung des Auftragsgebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Auftragsverarbeiters vorliegt.

(2) Die nachfolgenden Regelungen finden sowohl für den Auftragsverarbeiter als auch für alle in der Folge eingesetzten weiteren Auftragsverarbeiter entsprechende Anwendung.

(3) Der Auftragnehmer hat den weiteren Auftragsverarbeiter in dem Unterauftragsverarbeitungsvertrag ebenso zu verpflichten, wie auch der Auftragnehmer aufgrund dieses Vertrages gegenüber dem Auftraggeber verpflichtet ist. Dem Auftraggeber sind im Unterauftragsverarbeitungsvertrag gegenüber dem weiteren Auftragsverarbeiter unmittelbar sämtliche Kontrollrechte gemäß Ziffer 7 dieses Vertrages einzuräumen (echter Vertrag zugunsten Dritter). Der Auftragnehmer haftet für ein Verschulden jedes weiteren Auftragsverarbeiters wie für eigenes Verschulden.

(4) Der Auftraggeber ist berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers sowie auch Einsicht in die relevanten Vertragsunterlagen zu erhalten.

(5) Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der personenbezogenen Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

(6) Der Auftraggeber stimmt hiermit der Inanspruchnahme der weiteren Auftragsverarbeiter gemäß Anlage 1 zu.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, den Auftragnehmer vor dem Beginn der Verarbeitung von personenbezogenen Daten des Auftraggebers und regelmäßig während der Laufzeit des Hauptvertrages bezüglich der Einhaltung der Regelungen dieser Anlage, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen gemäß Anlage 2, selbst oder durch einen von ihm beauftragten Prüfer zu überprüfen; einschließlich Inspektionen. Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei, unter anderem durch die Gewährung der notwendigen Zugangs- und Zugriffsrechte sowie der Bereitstellung aller notwendigen Informationen.

(2) Der Auftragnehmer hat sicherzustellen und regelmäßig zu kontrollieren, dass die Verarbeitung der personenbezogenen Daten des Auftraggebers mit den Regelungen dieses Vertrages sowie den Weisungen des Auftraggebers in Einklang steht. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

☐ die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO;

☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfung, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 8 Mitteilung bei Verstößen des Auftragnehmers

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

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, jede potenzielle Verletzung des Schutzes der personenbezogenen Daten des Auftraggebers, insbesondere Vorkommnisse, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten des Auftraggebers führen können („Datensicherheitsvorfall“), unverzüglich, spätestens aber innerhalb von 24 Stunden, nachdem ihm eine solche bekannt geworden ist, 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) Der Auftragnehmer darf die personenbezogenen Daten des Auftraggebers ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. Im letzteren Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Mündliche Weisungen des Auftraggebers werden durch diesen unverzüglich bestätigt (mind. Textform).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung des Auftraggebers verstoße gegen diesen Vertrag oder das geltende Datenschutzrecht. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Bestätigt der Auftraggeber die Weisung, ist der Auftragnehmer verpflichtet, sie zu befolgen.

(4) Der Auftragnehmer ist verpflichtet, sämtliche Weisungen des Auftraggebers zu dokumentieren.

(5) Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind:

[Vorname, Name, Organisationseinheit, Telefon, E-Mail]

§ 10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht, unwiderruflich zu vernichten, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der personenbezogenen Daten des Auftraggebers besteht. 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 den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren und dem Auftraggeber auch nach Vertragsende auf Verlangen in Kopie herauszugeben.

§ 11 Haftung

(1) Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers gegen diesen Vertrag sowie gegen die ihn unmittelbar treffenden gesetzlichen Datenschutzverpflichtungen haftet der Auftragnehmer entsprechend den gesetzlichen Haftungsregelungen. Etwaige anderweitige zwischen den Parteien vereinbarte Haftungsbegrenzungen (z. B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung. Soweit Dritte Ansprüche gegen den Auftraggeber geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftragnehmers gegen diesen Vertrag oder gegen eine ihn unmittelbar treffende gesetzliche Datenschutzverpflichtungen haben, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen auf erstes Anfordern frei.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber auch von allen etwaigen Geldbußen, die gegen den Auftraggeber verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in denen der Auftragnehmer Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

(3) Der Auftragnehmer trägt die Beweislast dafür, dass etwaige Schäden und Geldbußen nicht auf einem von ihm zu vertretenden Umstand beruhen, soweit die jeweilige Ursache in der Verarbeitung von personenbezogenen Daten des Auftraggebers in der Zuständigkeitssphäre des Auftragnehmers liegt.

§ 12 Rechtswahl und Gerichtsstand

(1) Es gilt deutsches Recht.

(2) Gerichtsstand ist der Sitz des Auftraggebers.

§ 13 Salvatorische Klausel

(1) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.

(2) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrages vor.

(3) Änderungen, Ergänzungen oder eine Aufhebung dieses AVV bedürfen der Textform. Dies gilt auch für eine Regelung, mit der diese Textformklausel abbedungen wird. Die elektronische Form ist insoweit ausreichend.

§ 14 Sonstiges

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(3) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch

sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Unterschriften:

[Ort]

Auftragnehmer

Auftragnehmer*in	Auftragnehmer*in
Funktion	Head of Legal Department

[Ort]

Auftraggeber

Auftrageber*in	Auftraggeber*in

ANLAGEN

Anlage 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Anlage 2: Technische und organisatorische Maßnahmen

ANLAGE 1: UNTERAUFTRAGSVERHÄLTNIS BEIM AUFTRAGNEHMER ZUM ZEITPUNKT DER AUFTRAGSVERGABE

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung

ANLAGE 2: NACHWEIS DER ALLGEMEINEN TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

1. VERTRAULICHKEIT

1.1. ZUTRITTSKONTROLLE

☐ Es sind keine Maßnahmen zur Zutrittskontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Zutrittskontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Zutrittskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☐ Schlüsselregelung / Liste
☐ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Besucherprotokoll
☐ Chipkarten / Transpondersysteme	☐ Mitarbeiter- / Besucherausweise
☐ Manuelles Schließsystem	☐ Besucher in Begleitung durch Mitarbeiter
☐ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☐
☐ Absicherung der Gebäudeschächte	☐
☐ Türen mit Knauf Außenseite	☐
☐ Klingelanlage mit Kamera	☐
☐ Videoüberwachung der Eingänge	☐
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

1.2. ZUGANGSKONTROLLE

☐ Es sind keine Maßnahmen zur Zugangskontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Zugangskontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Zugangskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Login mit Benutzername und Passwort	☐ Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	☐ Erstellen von Benutzerprofilen
☐ Anti-Virus-Software Server	☐ Zentrale Passwortvergabe
☐ Anti-Virus-Software Clients	☐ Richtlinie „Sicheres Passwort“
☐ Anti-Virus-Software mobile Geräte	☐ Richtlinie „Löschen / Vernichten“
☐ Firewall	☐ Richtlinie „Clean Desk“
☐ Intrusion Detection Systeme	☐ Allgemeine Datenschutz- und / oder Sicherheitsrichtlinie
☐ Mobile Device Management	☐ Mobile Device Policy
☐ Einsatz VPN bei Remote-Zugriffen	☐ Anleitung „Manuelle Desktopsperre“
☐ Verschlüsselung von Datenträgern	☐
☐ Verschlüsselung von Smartphones	☐
☐ Gehäuseverriegelung	☐
☐ BIOS-Schutz (separates Passwort)	☐
☐ Sperre externer Schnittstellen (USB)	☐
☐ Automatische Desktopsperre	☐

☐ Verschlüsselung von Notebooks / Tablets	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

1.3. ZUGRIFFSKONTROLLE

☐ Es sind keine Maßnahmen zur Zugriffskontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Zugriffskontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Zugriffskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Aktenschredder (mind. Stufe 3, cross cut)	☐ Einsatz Berechtigungskonzepte
☐ Externer Aktenvernichter (DIN 32757)	☐ Minimale Anzahl an Administratoren
☐ Physische Löschung von Datenträgern	☐ Datenschutztresor
☐ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐ Verwaltung der Benutzerrechte durch Administratoren
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

1.4. TRENNUNGSKONTROLLE

☐ Es sind keine Maßnahmen zur Trennungskontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Trennungskontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Trennungskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung von Produktiv- und Testumgebung	☐ Steuerung über Berechtigungskonzept

☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☐ Festlegung von Datenbankrechten
☐ Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze mit Zweckattributen versehen
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

1.5. PSEUDONYMISIERUNG

☐ Es sind keine Maßnahmen zur Pseudonymisierung erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Pseudonymisierung, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Pseudonymisierung:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (ggf. verschlüsselt)	☐ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

2. INTEGRITÄT

2.1. WEITERGABEKONTROLLE

☐ Es sind keine Maßnahmen zur Weitergabekontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Weitergabekontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Weitergabekontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ E-Mail-Verschlüsselung	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ Einsatz von VPN	☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen
☐ Bereitstellung über verschlüsselte Verbindungen wie stfp, https	☐ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☐
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

2.2. EINGABEKONTROLLE

☐ Es sind keine Maßnahmen zur Eingabekontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Eingabekontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Eingabekontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Übersicht, mit welchem Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle

	Benutzernamen (nicht Benutzergruppen)
☐	☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	☐ Aufbewahren von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
☐	☐ Klare Zuständigkeiten für Löschungen
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

3. VERFÜGBARKEIT UND BELASTBARKEIT

3.1. VERFÜGBARKEITSKONTROLLE

☐ Es sind keine Maßnahmen zur Verfügbarkeitskontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Verfügbarkeitskontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Feuer- und Rauchmeldeanlagen	☐ Backup- und Recoverykonzept (ausformuliert)
☐ Feuerlöscher Serverraum	☐ Kontrolle des Sicherungsvorgangs
☐ Serverraumüberwachung Temperatur und Feuchtigkeit	☐ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☐ Serverraum klimatisiert	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☐ USV	☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐ Schutzsteckdosenleisten Serverraum	☐ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)

☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☐ Getrennte Partitionen für Betriebssysteme und Daten
☐ RAID System / Festplattenspiegelung	☐
☐ Videoüberwachung Serverraum	☐
☐ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

4.1. DATENSCHUTZMANAGEMENT

☐ Es sind keine Maßnahmen zum Datenschutzmanagement erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zum Datenschutzmanagement, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zum Datenschutzmanagement:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für Datenschutzmanagement im Einsatz	☐ Interner / Externer Datenschutzbeauftragter (siehe Nr. 5)
☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffs-möglichkeiten für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet)	☐ Mitarbeiter geschult und zu Vertraulichkeit / Datensparsamkeit verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☐ Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)
☐ Anderweitiges dokumentiertes Sicherheitskonzept: *[Nennung]*	☐ Interner / Externer Informationssicherheits-beauftragter: *[Nennung]*
☐ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☐ Eine Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt

☐	☐ die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
☐	☐ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

4.2. INCIDENT-RESPONSE-MANAGEMENT

☐ Es sind keine Maßnahmen zum Incident-Response-Management erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zum Incident-Response-Management, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zum Incident-Response-Management:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von Firewall und regelmäßige Aktualisierung	☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☐ Einsatz von Spamfilter und regelmäßige Aktualisierung	☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☐ Einsatz von Virenscanner und regelmäßige Aktualisierung	☐ Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	☐ Dokumentation von Sicherheitsvorfällen und Datenpannen z. B. mittels Ticketsystem
☐ Intrusion Prevention System (IPS)	☐ Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

4.3. DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

☐ Es sind keine Maßnahmen zu datenschutzfreundlichen Voreinstellungen erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zu datenschutzfreundlichen Voreinstellungen, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zu datenschutzfreundlichen Voreinstellungen:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☐ Einfache Ausübung des Widerrufrechts des Betroffenen durch organisatorische Maßnahmen
☐ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☐	☐
☐	☐

Weitere Maßnahmen sind: *[Nennung]*.

4.4. AUFTRAGSKONTROLLE

☐ Es sind keine Maßnahmen zur Auftragskontrolle erforderlich, weil *[Begründung]*.

☐ Es existieren keine Maßnahmen zur Auftragskontrolle, weil *[Begründung]*.

☐ Es existieren folgende Maßnahmen zur Auftragskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☐	☐ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
☐	☐ Schriftliche Weisungen an den Auftragnehmer

☐	☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐	☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☐ Regelung zum Einsatz weiterer Subunternehmer
☐	☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen sind: *[Nennung]*.