HELMHOLTZ MUNICH

Formblatt AVV – VgV_2024-054

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

VgV_2024-054 Software Arbeitssicherheit

Helmholtz Zentrum München
Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH)
Ingolstädter Landstr. 1
85764 Neuherberg

- nachstehend „**Auftraggeber**“ oder **„AG“** genannt -

und

_____
_____
_____

- nachstehend „**Auftragnehmer**“ oder **„AN“** genannt -

1. Gegenstand dieser Vereinbarung und Dauer

1.1 Der Auftraggeber (kurz: „**AG“**) hat den Auftragnehmer (kurz: „**AN“**) im Rahmen eines Vertrages mit der Erbringung verschiedener Leistungen (auch kurz: **„Services“**) beauftragt. Die hiesige Vereinbarung („**AV-Vereinbarung**“) ergänzt den Vertrag um Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO. Die genaue Bezeichnung des Vertrages findet sich in **Anlage 1** zur hiesigen AV-Vereinbarung.

1.2 Soweit der AN im Rahmen der Leistungserbringung personenbezogene Daten, die er vom AG erhält oder erhebt (kurz: **„Daten“**), verarbeitet und/oder mit der Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen des AG beauftragt ist, bei der für den AN die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, erfolgt dies ausnahmslos im Auftrag des AG und im Sinne einer Auftragsverarbeitung nach Art. 28 DSGVO (kurz: **„AV“**).

1.3 Der AG bleibt insofern datenschutzrechtlich Verantwortlicher, d. h. „Herr der Daten“ und im Verhältnis zu den Betroffenen für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

1.4 Die hiesige AV-Vereinbarung regelt die Details der AV gemäß Art. 28 und Art. 29 DSGVO und geht betreffend die Verarbeitung der Daten durch den AN allen anderen Regelungen zwischen den Parteien vor. Sie ersetzt betreffend die Verarbeitung der Daten im Auftrag zugleich alle gegebenenfalls bestehenden älteren AV-Vereinbarungen (inklusive Vereinbarungen nach § 11 BDSG).

1.5 Beginn, Dauer, Ende und Kündigungsmöglichkeiten der AV-Vereinbarung entsprechen denjenigen des Vertrags. Soweit es dort dazu keine Regelungen gibt, gilt das Folgende: Die AV beginnt mit der Unterzeichnung der hiesigen AV-Vereinbarung und läuft unbefristet; sie kann von beiden Parteien mit einer Frist von vier Wochen zum Ende eines Monats schriftlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund (s. Ziff. 9.1) bleibt unberührt. Sofern ein wichtiger Grund zur außerordentlichen Kündigung dieser AV-Vereinbarung vorliegt, begründet dieser zugleich einen wichtigen Grund zur außerordentlichen Kündigung des Vertrages.

2. Einzelheiten zur Datenverarbeitung durch den AN im Auftrag des AG

2.1 Die datenschutzrechtlichen Details betreffend der vom AN zu erbringenden Services sind in **Anlage 1** dergestalt festgelegt, dass dort für jeden Service beschrieben ist:

(1) Gegenstand, Art und Zweck der im Rahmen der Serviceerbringung erfolgenden Verarbeitung von personenbezogenen Daten,
(2) die Art der dabei verarbeiteten personenbezogenen Daten und
(3) die jeweiligen Kategorien der von dieser Datenverarbeitung Betroffenen.

2.2 Der AN verarbeitet die Daten ausschließlich im Rahmen dieser AV-Vereinbarung, insbesondere im Umfang nach den relevanten Vorgaben der **Anlage 1**, sowie etwaiger dokumentierter Einzelweisungen des AG nach Ziffer 2.3; Abweichungen sind nicht zulässig.

Zu anderen Verarbeitungen der Daten ist der AN insofern nur berechtigt, soweit er hierzu nach dem Recht der EU oder des EU-Staats, dem er unterliegt, gesetzlich verpflichtet ist; in einem solchen Fall teilt der AN diese rechtlichen Anforderungen dem AG vor der Verarbeitung schriftlich mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Mit Ausnahme vorstehend gesetzlicher Verpflichtungen darf der AN die Daten nicht zu anderen, insbesondere nicht zu eigenen Zwecken verwenden und keine Kopien oder Duplikate hiervon anfertigen.

2.3 Einzelweisungen des AG müssen sich im Rahmen des vertraglich vereinbarten Leistungsumfangs halten. Einzelweisungen hat der AG schriftlich zu erteilen. Bei Gefahr in Verzug kann der AG eine Einzelweisung auch mündlich erteilen, der AG hat diese im Anschluss unverzüglich in Schriftform zu bestätigen. Der AN wird den AG unverzüglich informieren, wenn eine Einzelweisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. Der AN ist dann berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den AG nach Überprüfung bestätigt oder geändert wird.

2.4 Der AN darf die Daten nur auf Einzelweisung des AG oder soweit dies Teil der Leistung nach **Anlage 1** ist berichtigen, löschen oder deren Datenverarbeitung einschränken. Zum Löschen hat der AN sichere Methoden nach dem Stand der Technik einzusetzen, die der AN dem AG auf Aufforderung nachzuweisen hat.

2.5. Sollte sich ein Betroffener wegen einer datenschutzrechtlichen Auskunft oder anderer ihm zustehenden Betroffenenrechte unmittelbar an den AN wenden, hat der AN den AG darüber unverzüglich zu informieren und vor jeglicher weiteren Tätigkeit und Kommunikation dessen Einzelweisung abzuwarten.

2.6. Der AN sichert zu, dass er Zugang und Zugriff auf die Daten streng auf die Personen begrenzt, die zur Erbringung der Services auf die Daten zugreifen müssen. Der AN sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Personen vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht und für die Zeit ihrer Tätigkeit wie auch im Anschluss in geeigneter Weise zur Verschwiegenheit und dazu verpflichtet hat, die Daten nicht unbefugt zu verarbeiten. Zum Nachweis der Erfüllung dieser Pflicht wird der AN dem AG auf dessen Aufforderung entsprechende Nachweise übersenden, insbesondere Kopien der Verpflichtungserklärungen.

2.7 Der AN kontrolliert und dokumentiert bei sich und bei von ihm eingesetzten Unterauftragnehmern regelmäßig die korrekte Verarbeitung der Daten und die Einhaltung der datenschutzrechtlichen Vorschriften durch die jeweiligen Mitarbeiter sowie die Erfüllung der Pflichten aus dieser AV-Vereinbarung. Er weist dem AG auf dessen Aufforderung vorgenommene Kontrollen schriftlich nach und legt deren Dokumentation vor. Der AN stellt ferner sicher, dass bei ihm alle Verarbeitungstätigkeiten, die er im Rahmen der AV-Vereinbarung für den AG durchführt, gemäß Art. 30 Abs. 2 DSGVO dokumentiert sind. Auf Anforderung des AG stellt der AN dem AG diese Dokumentation zur Verfügung.

2.8 Der AN erstattet dem AG unverzüglich schriftlich und unter Angabe von Details Meldung bei

(1) Verdacht auf Verletzungen des Schutzes personenbezogener Daten,
(2) Verstöße durch ihn oder seine Mitarbeiter, Unterauftragnehmer oder Dritte gegen Datenschutz-Vorschriften oder gegen die im Auftrag getroffenen Festlegungen,
(3) Abweichungen der technischen und organisatorischen Maßnahmen des AN von den mit dem AG vereinbarten Anforderungen,
(4) Unregelmäßigkeiten bei der Verarbeitung von Daten,
(5) jeglichem unautorisierten Zugriff oder einer unautorisierten Verarbeitung von Daten und/oder
(6) Anfragen, Kontrollhandlungen, Untersuchungen oder anderen Maßnahmen einer Aufsichtsbehörde für den Datenschutz oder einer anderen Behörde (z. B. Polizei oder Gericht) beim AN.

Die Meldung hat durch den AN beim AG spätestens binnen 24 Stunden zu erfolgen, nachdem dem AN die Verletzung, Abweichung oder Unregelmäßigkeit bekannt wurde.
Vorstehende Meldepflichten gelten vor allem auch im Hinblick auf eventuelle eigene Melde- und Benachrichtigungspflichten des AG nach Art. 33 und Art. 34 DSGVO. Der AN sichert zu, den AG insofern bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen, wie zum Beispiel dem AG sachkundige Ansprechpartner zur Seite zu stellen, relevante Unterlagen zugänglich machen und Fragen des AG beantworten.

Meldungen nach Art. 33 oder 34 DSGVO für den AG darf der AN nicht vornehmen, es sei denn, es liegt insofern eine ausdrückliche Einzelweisung des AG vor.

2.9 Meldungen des AN nach Ziffer 2.8. enthalten

(1) eine Beschreibung der Art der Verletzung, Abweichung oder Unregelmäßigkeit, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen Datensätze;

(2) eine Beschreibung der wahrscheinlichen Folgen der Verletzung, Abweichung oder Unregelmäßigkeit; und

(3) eine Beschreibung der vom AN ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung, Abweichung oder Unregelmäßigkeit und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

2.10 Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten (**„DSB“**) des AN sowie weitere Angaben des AN zu seiner Datenschutz-Organisation sind in **Anlage 2** festgelegt. Besteht keine Pflicht zur Bestellung eines DSB, hat der AN eine andere Anlaufstelle für den Datenschutz beim AN zu benennen. Ein Wechsel des DSB, der Anlaufstelle oder sonstige Änderungen der Angaben in **Anlage 2** hat der AN dem AG unverzüglich in Schriftform mitzuteilen.

2.11 Der AN unterstützt betreffend die Daten den AG mit geeigneten technischen und organisatorischen Maßnahmen, den Betroffenenrechte nach Art. 12 bis 23 DSGVO nachzukommen sowie bei der Einhaltung der in Art 32 bis 36 DSGVO genannten Pflichten des AG hinsichtlich der Sicherheit personenbezogener Daten sowie einer ggf. erforderlichen Datenschutz-Folgenabschätzung und vorherigen Konsultationen der Aufsichtsbehörden. Der AN hat dem AG darüber hinaus auf dessen Anforderung alle Auskünfte und Informationen zur Verfügung zu stellen, die der AG zur Erfüllung sonstiger ihn treffender gesetzlichen Vorgaben benötigt (etwa zur Erstellung des Verzeichnisses von Verarbeitungstätigkeiten).

2.12 Der AN sichert zu, dass die Daten von sonstigen Datenbeständen (eigene des AN oder von anderen Kunden des AN) strikt getrennt werden; weitere Details dazu sind in der **Anlage 5** unter dem Stichwort „Vertraulichkeit – Trennungskontrolle“ beschrieben. Datenträger, die vom AG stammen bzw. für den AG genutzt werden, kennzeichnet der AN besonders und dokumentiert deren Eingang und Ausgang sowie die laufende Verwendung.

3. Ort der Datenverarbeitung durch den AN

3.1 Der AN verarbeitet die Daten nur in einem Mitgliedsstaat der Europäischen Union (EU) oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR); maßgeblich ist dabei der Status des Landes im Zeitpunkt der jeweiligen Verarbeitung. Dies gilt auch für bloße Zugriffe auf die Daten von solchen Ländern aus.

3.2 Soweit der AN (siehe zu Unterauftragnehmern Ziffer 4.) dagegen die Daten nicht im Gebiet der EU/EWR verarbeitet oder von außerhalb dieses Gebiets auf die Daten zugreift, ist dies nur zulässig, wenn

- die besonderen Voraussetzungen der Artt. 44 ff DSGVO erfüllt sind (siehe dazu Anlage 3) und der AN dies dem AG nachweist; und
- der AG dem ausdrücklich zugestimmt hat, entweder dadurch, dass Anlage 3 zum Zeitpunkt des Abschlusses der AV-Vereinbarung vollständig und korrekt ausgefüllt ist oder bei späterer Verlagerung der Datenverarbeitung in ein Gebiet außerhalb der EU/EWR durch gesonderte Ausfertigung der **Anlage 3** und der dort schriftlich vom AG erklärten vorherigen Zustimmung zu dieser Verlagerung.

3.3 Die Daten dürfen vom AN nur in dessen Geschäftssitz sowie dessen geschäftlichen Niederlassungen verarbeitet werden. Ein Zugriff auf die Daten von außerhalb (etwa bei Telearbeit, Homeoffice, mobilen Arbeiten o. Ä.) ist nur zulässig, sofern der AN durch geeignete technische und organisatorische Maßnahmen sicherstellt, dass das Datenschutz- und Datensicherheitsniveau nicht beeinträchtigt wird; dies können z. B. VPN-Verbindungen und die ausschließliche Nutzung von Endgeräten, die der AN seinen Mitarbeitern zur Verfügung gestellt hat, sein. Zudem wird vorausgesetzt, dass der AN auch am Ort des externen Zugriffs Zutritt zur Durchführung von Kontrollen, wie nach dieser Vereinbarung vorgesehen, hat sowie für die Einhaltung der Vorgaben dieser AV-Vereinbarung inkl. deren Anlagen sorgt. Dies hat der AN mit seinen Mitarbeitern vertraglich sicherzustellen.

4. Einschaltung von Unterauftragnehmern

4.1 Der AN darf sich bei der Leistungserbringung Unterauftragnehmern nur mit vorheriger und schriftlicher ausdrücklicher Zustimmung des AG bedienen.

4.2 Mit den in **Anlage 4** genannten Unterauftragnehmern besteht seitens des AG Einverständnis.

Weitere Unterauftragnehmer, deren Einsatz der AG nach den Regelungen dieser AV-Vereinbarung zugestimmt hat, hat der AN in die **Anlage 4** aufzunehmen und dem AG als aktualisierte Fassung zu übersenden.

4.3 Soweit mit entsprechender Zustimmung des AG der AN ausnahmsweise Unterauftragnehmer mit Sitz außerhalb der EU bzw. des EWR einschalten darf, muss der AN dabei zwingend die Voraussetzungen der Art. 44 bis 49 DSGVO einhalten und dies dem AG nachweisen. Soweit der AG aufgrund aktueller Datenschutzvorgaben dabei gegebenenfalls Standarddatenschutzklauseln direkt mit dem Subunternehmer abzuschließen hat, unterstützt der AN den AG dabei und tritt diesen Klauseln gegebenenfalls selbst mit bei.

4.4 Der AN hat in jedem Fall seine Verträge mit Unterauftragnehmern so zu gestalten, dass sie datenschutzrechtlich mindestens den Datenschutzbestimmungen der hiesigen AV-Vereinbarung und Art. 28 und Art. 29 DSGVO entsprechen, die Verantwortlichkeiten zwischen AN und dem jeweiligen Unterauftragnehmer klar voneinander abgegrenzt sind und der AG dieselben Rechte auch direkt gegenüber dem jeweiligen Unterauftragnehmer hat, wie er sie nach dieser AV-Vereinbarung gegenüber dem AN hat. Dies umfasst insbesondere direkte Kontrollrechte des AG bei dem jeweiligen Unterauftragnehmer. Die Vereinbarung zwischen dem AN und einem Unterauftragnehmer muss außerdem hinreichende Garantien dafür bieten, dass vom jeweiligen Unterauftragnehmer die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser AV-Vereinbarung und der einschlägigen Datenschutzgesetze erfolgt.

4.5 Der AN ist im Verhältnis zum AG für die bestmögliche und datenschutzkonforme Auswahl von geeigneten Unterauftragnehmern sowie die jeweils dort erfolgende datenschutzkonforme Verarbeitung der Daten verantwortlich. Der AN muss seine Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählen. Der AN ist ferner verpflichtet, die Einhaltung der Pflichten bei sämtlichen Unterauftragnehmern regelmäßig zu prüfen und zu dokumentieren. Auf Anfrage des AG hat der AN ihm die für die Auswahlprüfung und die regelmäßige Prüfung relevanten Prüfunterlagen zu übersenden.

4.6 Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der AN gegenüber dem AG für die Einhaltung der Pflichten jenes Unterauftragnehmers wie für eigene Pflichtverletzungen. Die Haftung des AN für seine eigenen Verpflichtungen im Zusammenhang mit dem Unterauftragnehmer bleibt davon unberührt.

4.7 Die Weiterleitung von Daten an Unterauftragnehmer oder deren Zugriff darauf ist erst dann zulässig, wenn der AN die Voraussetzungen nach dieser Vereinbarung sowie Art. 28 DSGVO geschaffen hat sowie der jeweilige Unterauftragnehmer seinen Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Mitarbeiter nachgekommen ist.

4.8 Die Regelungen dieser Ziffer 4 gelten auch für sämtliche von Unterauftragnehmer eingeschalteten weiteren Unterauftragnehmer, ebenso wie von diesen wiederum eingeschalteten weiteren Unterauftragnehmern (usw.) in der gesamten Kette.

5. Vom AN getroffene technische und organisatorische Schutzmaßnahmen

5.1 Der AN hat die Sicherheit der Verarbeitung gem. Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Der AN gewährleistet insofern für die Erbringung der Leistungen ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau. Dazu berücksichtigt der AN die Schutzziele von Art. 32 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart, dass durch geeignete technische und organisatorische Maßnahmen das Risiko auf Dauer möglichst ausgeschlossen wird.

5.2 Das in **Anlage 5** beschriebene Datenschutzkonzept legt die Auswahl der technischen und organisatorischen Maßnahmen (kurz: „**TOM**“) passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem

Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim AN fest. Der AN ist verpflichtet, die TOM während der Laufzeit dieser AV-Vereinbarung aufrecht zu erhalten. Er beachtet zudem die Grundsätze der ordnungsgemäßen Datenverarbeitung.

5.3 Im Rahmen des technischen Fortschritts und der Weiterentwicklung ist es dem AN gestattet und er zugleich im Falle technischer Notwendigkeit verpflichtet, einzelne TOM anzupassen, soweit es sich um adäquate Maßnahmen handelt und zugleich das Sicherheitsniveau der in **Anlage 5** festgelegten TOM nicht unterschritten wird. Auf Aufforderung des AG informiert der AN den AG über solche Änderungen, wesentliche Änderungen sind dagegen vor ihrer Einführung einvernehmlich festzulegen.

6. Kontrollen des AG

6.1 Der AN erklärt sich damit einverstanden, dass der AG jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz, dieser AV-Vereinbarung samt ihren Anlagen, insbesondere auch der vereinbarten TOM nach **Anlage 5,** selbst oder durch Dritte zu kontrollieren, insbesondere durch Einholung von Auskünften und die Einsichtnahme in gespeicherte Daten und die Datenverarbeitungsprogramme sowie Kontrollen beim AN vor Ort. Der AG ist insofern verpflichtet, alle erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des AN vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

6.2 Der AN sichert zu, dass er, soweit erforderlich, bei Kontrollen des AG jeweils mitwirkt und den AG unterstützt, ihm insbesondere Zutritt gewährt sowie Unterlagen zur Verfügung stellt (Protokolle, Berichte des Datenschutzbeauftragten, Zertifizierungen etc.).

7. Beendigung der AV

7.1 Auf jederzeit mögliche Aufforderung des AG, spätestens aber mit Beendigung der AV, hat der AN unverzüglich dem AG dessen Daten in einem für den AG lesbaren gängigen elektronischen Format herauszugeben oder auf gesonderte Einzelweisung diese Daten bei sich datenschutzkonform physikalisch zu löschen. Der AN hat den AG spätestens binnen 2 Wochen nach Beendigung der AV aufzufordern, vorstehendes Wahlrecht auszuüben. Vorstehende Regelungen gelten entsprechend für personenbezogenes Test- und Ausschussmaterial.

7.2 Löschungen nach vorstehenden Absatz hat der AN zu protokollieren und das Löschprotokoll dem AG unverzüglich zuzusenden und dort die Vollständigkeit der Datenlöschung sowie die Richtigkeit der Angaben schriftlich zu bestätigen.

7.3 Dokumentationen des AN, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung durch den AN dienen, sowie Unterlagen, die gesetzlichen Aufbewahrungspflichten des AN unterliegen, sind im jeweils erforderlichen Umfang von vorstehenden Regelungen ausgenommen. Soweit dort Daten enthalten sind, hat der AN den AG spätestens mit Beendigung der AV-Vereinbarung zu informieren.

8. Haftung und wechselseitige Information

8.1 Der AN haftet nach den gesetzlichen Haftungsregelungen für Schäden, die beim AG durch Verstöße des AN gegen diese Vereinbarung und/oder der gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen entstehen. Bußgelder gelten auch als solche Schäden.

Etwaige Haftungsbegrenzungen aus dem jeweiligen Vertrag über die Erbringung der betroffenen Services finden keine Anwendung.

8.2 Soweit im Zusammenhang mit der nach dieser AV-Vereinbarung erfolgenden Datenverarbeitung gegen AN oder AG Schadensersatzansprüche (Art. 82 DSGVO), Geldbußen (Art. 83 DSGVO) oder andere Sanktionen (Art. 84 DSGVO) angedroht oder geltend gemacht werden, haben sich AN und AG darüber jeweils unverzüglich wechselseitig zu informieren. Ohne vorherige Abstimmung mit der jeweils anderen Partei darf die jeweils betroffene Partei keine Stellungnahmen sowie kein Anerkenntnis oder eine vergleichbare Erklärung abgeben; werden sich AN und AG betreffend die Art und Weise der Abwehr nicht einig, liegt das Letztentscheidungsrecht beim AG als „Herr der Daten“. Zudem haben sich beide Parteien bei der Anspruchsabwehr zu unterstützen.

9. Sonstige Bestimmungen

9.1 Der AG kann die AV-Vereinbarung und den zugrundeliegenden vertraglichen Auftrag jederzeit außerordentlich ohne Einhaltung einer Frist kündigen, wenn der AN schwerwiegend gegen Datenschutzvorschriften oder die Bestimmungen dieser AV-Vereinbarung verstößt, eine nach dieser AV-Vereinbarung zu befolgende Weisung des AG trotz Mahnung nicht ausführt oder dem AG Kontrollrechte vertragswidrig verweigert.

9.2. Die Einrede des Zurückbehaltungsrechts nach § 273 BGB an den Daten, Teilen davon sowie Datenträgern des AG wird ausgeschlossen.

9.3 Soweit die Daten beim AN durch Beschlagnahme oder Pfändung, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der AN den AG unverzüglich darüber zu informieren. Der AN hat alle in diesem Zusammenhang Beteiligten zu informieren, dass ausschließlich der AG Verantwortlicher und „Herr der Daten“ ist.

9.4 Eine gesonderte Vergütung für Tätigkeiten des AN, insbesondere Unterstützungsleistungen, nach dieser AV-Vereinbarung fällt nicht an, diese ist vielmehr mit der Vergütung aus dem Vertrag abgegolten.

9.5 Änderungen oder Ergänzungen der AV-Vereinbarung oder ihrer Bestandteile und Anlagen – einschließlich etwaiger Zusicherungen des AN – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung oder Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Schriftform im vorstehenden Sinne bedeutet die Form des § 126 BGB

9.6 Gesetzliche Regelungen im Sinne dieser AV-Vereinbarung umfassen auch Verordnungen der EU.

9.7 Mit Ausnahme von Ziffer 9.5 genügt zur Einhaltung der Schriftform im Sinne dieser AV-Vereinbarung auch die Textform (wie etwa E-Mail).

9.8 Für die AV-Vereinbarung gilt das Recht der Bundesrepublik Deutschland, soweit nicht die DSGVO vorrangige Regelungen enthält. Soweit im Vertrag ein Gerichtsstand vereinbart wurde, gilt diese Vereinbarung auch für alle Ansprüche oder Angelegenheiten, die sich aus oder im Zusammenhang mit dieser AV-Vereinbarung ergeben.

9.9 Sollten einzelne Teile dieser AV-Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der AV-Vereinbarung im Übrigen nicht.

10. Anlagen

Folgende Anlagen sind verbindlicher Teil dieser AV-Vereinbarung:

Anlage 1:	Details zur Auftragsverarbeitung
Anlage 2:	Angaben zur Datenschutz-Organisation des AN
Anlage 3:	Ort der Datenverarbeitung durch AN außerhalb EU/EWR
Anlage 4:	Liste von genehmigten Unterauftragnehmern
Anlage 5:	Beschreibung der vom AN zum Schutz der Daten des AG getroffenen technischen und organisatorischen Maßnahmen

11. Unterschriften

Auftraggeber	Auftragnehmer
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Funktion und Name in Druckbuchstaben	Funktion und Name in Druckbuchstaben
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlage 1: Details zur Auftragsverarbeitung

1. In Bezug genommener Vertrag für die Services der nachfolgenden Tabelle

   Bezeichnung des Vertrags: _____ Ggfls. Abschlussdatum: _____

2. Tabelle zu den Services und der damit verbundenen Verarbeitung von Daten des AG

Lfd. Nr.	Kurzbeschreibung der Leistungen/Services, die der AN für den AG erbringt (in Kurzform)	Gegenstand, Art und Zweck der diesbezüglichen Verarbeitung von personenbezogenen Daten (welche Leistungen betreffend die personenbezogenen Daten sind im Einzelnen zu erbringen: Erheben? Speichern? Übermitteln? Wie? etc.)	Speichert der AN bei sich die Daten des AG? Wann erfolgt Löschung?	Kreis der Betroffenen (= die Personengruppen, deren Daten verarbeitet werden) (Beispiele: Mitarbeiter des AG, Endkunden des AG, Azubis des AG etc.)	Art der personenbezogenen Daten, die der AN erhält/verarbeitet (= Kategorie der Daten, wie etwa „Adressdaten“ oder „Bestelldaten“ etc.)	Ort (Stadt/Land), an dem der AN die Daten verarbeitet	Weisungsberechtigte Funktionen auf Seiten des AG	Weisungsempfänger auf Seiten AN
	BEISPIEL: Druck von Visitenkarten von Mitarbeitern des AG	*BEISPIEL: Es sind die zu druckenden personenbezogenen Daten vom AN entgegenzunehmen und aus technischen Zwecken zwischen zu speichern. Diese werden dann für den Druck der Visitenkarten verarbeitet und gedruckt.*	*BEISPIEL: Ja. Löschung erfolgt nach Übersendung der gedruckten Visitenkarten an den AG und dessen Freigabe der Karten*	*BEISPIEL: Mitarbeiter des AG*	*BEISPIEL: Name und berufliche Kontaktdaten der Mitarbeiter*	*BEISPIEL: München*	*Beispiel: Direktor HR*	*Beispiel: Key Account Manager*

Anlage 2: Angaben zur Datenschutz-Organisation des AN

a. Datenschutzbeauftragter

☐ Beim AN ist ein Datenschutzbeauftragter bestellt (DSB). Name und Kontaktdaten: _____

☐ Es ist kein DSB bestellt. Grund: _____

b. Verschwiegenheit u.a.

Sind alle Mitarbeiter des ANs, die mit personenbezogenen Daten des AGs in Berührung kommen können, über die für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht, zur Verschwiegenheit und dazu verpflichtet, die Daten nicht unbefugt zu verarbeiten?

☐ Ja ☐ Nein, Grund: _____

c. Datenschutzschulungen

In welcher Weise werden die Mitarbeiter des ANs, die mit personenbezogenen Daten des AGs in Berührung kommen können, im Datenschutz geschult?

Art der Schulung: ☐ Präsenzschulung ☐ Web-based-Training ☐ Sonstiges: _____

Datum der letzten Schulung: _____ Inhalt der letzten Schulung: _____

d. Interne Datenschutzkontrollen

Der AN führt die folgenden internen Datenschutz-Kontrollen durch: _____

Was wird kontrolliert? _____ In welcher Weise? _____

Wie häufig? _____ Wann erfolgte die letzte Kontrolle? _____

Was war deren Ergebnis? _____

e. Zertifizierungen

Der AN verfügt über die folgenden Zertifikate/Testate (zum Beispiel ISO 27001 Zertifikat), welche auch oder im speziellen die Verfahren zur Erhebung, Verarbeitung oder Nutzung der Daten des AGs betreffen.

☐ Keine

☐ Folgende _____ ☐ Ja, Kopie anbei ☐ Nein, keine Kopie, da _____

_____ ☐ Ja, Kopie anbei ☐ Nein, keine Kopie, da _____

_____ ☐ Ja, Kopie anbei ☐ Nein, keine Kopie, da _____

f. Löschkonzept

Es liegt die Daten des AG betreffend ein Löschkonzept des AN bei.

☐ Ja ☐ Nein, Grund: _____

Anlage 3: Ort der Datenverarbeitung durch den AN außerhalb der EU/ EWR

Erfolgt die Datenverarbeitung durch den AN in oder aus einem Mitgliedstaat der EU oder EWR:

☐ Ja ☐ Nein

Wenn „Nein“, aus welchem Land ansonsten: _____

Name und Anschrift des vom AN für die EU benannten Vertreters: _____

Ein ausreichendes Datenschutz-Niveau in diesem Nicht-EU/Nicht-EWR-Land

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

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

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

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

☐ wird hergestellt durch die EU-Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO);
diese liegen in Form der controller-to-processor-Variante (MODUL ZWEI) als Kopie samt Anhängen anbei vor. Die EU-Standardverträge gehen bei Widersprüchen und Zweifeln stets den Regelungen der hiesigen AV-Vereinbarung vor.

Anlage 4: Liste von genehmigten Unterauftragnehmern

Werden Unterauftragnehmer eingesetzt? ☐ Nein ☐ Ja, siehe dann im Folgenden

Soweit Unterauftragnehmer eingesetzt werden, sind diese abschließend in folgender Tabelle aufzulisten; gleiches gilt für Unter-Unterauftragnehmer (usw.):

Lfd. Nr.	Name des Unterauftragnehmers	Anschrift des Unterauftragnehmers	Aufgabe des Unterauftragnehmers (= Welche personenbezogene Daten des AG verarbeitet der Unterauftragnehmer/ hat Zugriff aus welchen Gründen?)	Dortiger Datenschutzbeauftragter: Name und Kontaktdaten	Ort, an dem der Unterauftragnehmer die Daten verarbeitet	<u>Audits:</u> Wann erfolgte durch den AN das letzte Audit des AN? Was war dessen Ergebnis? Wann erfolgt das nächste Audit?	Setzt der Unterauftragnehmer „Unter-Unterauftragnehmer“ ein? Wenn ja: Bitte hier die entsprechenden (siehe die Spalten links) Angaben pro Unter-Unterauftragnehmer eintragen (Name, Adresse, Aufgabe, DSB, Ort) Gleiches gilt, wenn der Unter-Unterauftragnehmer weitere „Unter-Unter-Unterauftragnehmer“ (usw.) einsetzt.

Anlage 5: Beschreibung der vom AN zum Schutz der Daten des AG getroffenen technischen und organisatorischen Maßnahmen

Kurzbezeichnung	Erläuterung und Beispiele	*Beschreibung der konkret vom AN getroffenen Maßnahmen* *Wichtiger Ausfüll-Hinweis:* *Der AN hat konkret und im Detail (nur) die Maßnahmen zu beschreiben, die er zum Schutz der Daten getroffen hat, die er vom AG erhält/ auf die er Zugriff erhält:* *- Die Nennung nur von Schlagworten, wie etwa „Videoüberwachung" o.Ä., reicht nicht aus.* *- Es ist die Nennung von Details nötig, also im Beispiel: „Videoüberwachungssystem, bestehend aus X Kameras, die den Empfangs-, Eingangs- und Serverraum-Bereich überwachen, aufzeichnen und regelmäßig ausgewertet werden" o. Ä.)* *Werden die Daten des AG beim AN auf mehreren Systemen gespeichert, etwa auf dessen Server gespeichert und auf Desktop-PCs/ Clients verarbeitet, sind vom AN sowohl für die Server wie auch die Desktops die jeweils dazu getroffenen Maßnahmen zu beschreiben, etwa „a. Maßnahmen betreffend Server (…), b. Maßnahmen betreffend Clients (…)". Soweit Daten auf Notebook oder anderen mobilen Devices verarbeitet werden, ist dies aufgrund dort zu treffender erhöhter Maßnahmen eine dritte Kategorie (c. Maßnahmen auf mobile Devices).*
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)		
Zutrittskontrolle	Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen	
Zugangskontrolle	Keine unbefugte Systembenutzung, z. B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern	
Zugriffskontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen	
Trennungskontrolle	Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sandboxing	
Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)	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 entsprechende technischen und organisatorischen Maßnahmen unterliegen	
2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)		
Weitergabekontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur	
Eingabekontrolle	Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement	
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)		
Verfügbarkeitskontrolle	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	
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort, Erstellen eines Backup- & Recoverykonzepts, Testen von Datenwiederherstellung, Erstellen eines Notfallplans	
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)		
Datenschutz-Management	Regelmäßige Schulung der Mitarbeiter zum Datenschutz, schriftliche Bestellung eines Datenschutzbeauftragten, Verzeichnis der Verarbeitungstätigkeiten und Datenschutzkonzept ist vorhanden, Standards für die IT-Sicherheit (IT Grundschutz BSI, ISO 27001 etc.), Datenschutz-Folgenabschätzungen werden durchgeführt	
Incident-Response-Management	Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne, Konzept zur Meldung von Datenpannen an den Auftraggeber, internes Incident-Response-Management-Konzept vorhanden	

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	Treffen geeigneter Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden, Z. B. keine vorbelegten Auswahlfelder, Opt-in statt Opt-out	
Auftragskontrolle	Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen	