Deutscher Akademischer Austauschdienst
German Academic Exchange Service

Vertrag zur Auftragsverarbeitung

Der
Deutsche Akademische Austauschdienst e.V., Kennedyallee 50, 53175 Bonn

- Verantwortlicher -

und
die Firma [**Name und Kontaktdaten des/der Auftragsverarbeiter(s)**]

- Auftragsverarbeiter -

schließen zur Erfüllung der Anforderungen gemäß Artikel 28 Datenschutz-Grundverordnung (DSGVO)[1] diesen Vertrag inklusive seiner nachfolgenden verbindlichen Anlagen, wobei sich der Gegenstand und Zweck der Verarbeitung aus dem schriftlichen Hauptvertrag

Rahmenvereinbarung zur Durchführung von Englischkursen im Vereinigten Königreich (UK) für Lehrende an deutschen Hochschulen,
Vergabe-Nr. 100/2026 vom [Datum des Zuschlags] ergibt.

Anlage 1 Beschreibung der Verarbeitung

Anlage 2 Ansprechpartner und Weisungen des Verantwortlichen

Anlage 3 Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Anlage 4 Unterauftragsverarbeiter

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

1. Begriffsbestimmungen, Vorrangklausel

1.1. Es gelten die Begriffsbestimmungen der DSGVO.

1.2. Bei etwaigen Widersprüchen zwischen diesem Vertrag und etwaigen anderen Verträgen zwischen den Parteien gehen die Regelungen dieses Vertrags vor.

2. Rechte und Pflichten des Verantwortlichen

Der Verantwortliche ist insbesondere für die Rechtmäßigkeit der Verarbeitung gemäß Artikel 6 Absatz 1 DSGVO oder anderweitiger einschlägiger Rechtsgrundlagen, die Einhaltung des für ihn anwendbaren und verbindlichen Datenschutzrechts der Mitgliedstaaten sowie die Wahrung der Rechte der betroffenen Personen nach den Artikeln 7, 12 bis 22 DSGVO verantwortlich.

3. Weisungsgebundene Verarbeitung und Remonstrationspflicht

3.1. Für Weisungen des Verantwortlichen gegenüber dem Auftragsverarbeiter[2] (Artikel 29 i. V. m. Artikel 28 Absatz 3 Buchstabe a DSGVO) sind die in **Anlage 2** aufgeführten Ansprechpartner zuständig. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Im Rahmen einer Weisung kann für den Auftragsverarbeiter ein Ermessensspielraum bestehen bleiben, mit welchen geeigneten technischen und organisatorischen Maßnahmen die Weisung umgesetzt wird. Darüber hinaus erfolgt die Verarbeitung durch den Auftragsverarbeiter gemäß etwaiger in **Anlage 2** festgelegter Weisungen.

Bearbeitungshinweis: *Bitte mindestens eine der beiden Optionen auswählen. Die nicht gewählte Option kann entfernt werden.*

[2] Dieses Vertragsmuster findet regelmäßig nur Anwendung für Auftragsverarbeiter, die in einem EWR-Mitgliedstaat belegen sind oder in einem Drittland, für das gemäß Artikel 45 DSGVO ein Angemessenheitsbeschluss der EU-Kommission vorliegt. Ansonsten könnten ggf. die Standarddatenschutzklauseln der EU-Kommission gemäß Artikel 46 Abs. 2 DSGVO verwendet werden.

3.2. Weisungen werden vom Verantwortlichen grundsätzlich in Textform (z. B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom

☒ Auftragsverarbeiter

☐ Verantwortlichen

entsprechend in Textform (z. B. per E-Mail) bestätigt. Der Auftragsverarbeiter stellt sicher, dass alle erteilten Weisungen des Verantwortlichen seinen insoweit zuständigen Beschäftigten zugehen (z. B. durch zentrale Ablage aller Weisungen).

3.3. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf hinweisen, wenn die Befolgung einer vom Verantwortlichen erteilten Weisung nach seiner Ansicht gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt (Remonstrationspflicht). In diesem Fall kann er die Umsetzung der Weisung aussetzen, bis der Verantwortliche mitteilt, ob er an der Weisung festhält, diese anpasst oder aufhebt.

4. Vertraulichkeits-/ Verschwiegenheitspflicht

Der Auftragsverarbeiter wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Insoweit stellt der Auftragsverarbeiter sicher, dass diese Personen nur im Rahmen der Erforderlichkeit auf personenbezogene Daten der beauftragten Verarbeitungstätigkeit zugreifen („Need to know“). Soweit der Verantwortliche gesetzlichen Geheimhaltungspflichten unterliegt, verpflichtet der Auftragsverarbeiter die zur Durchführung des Auftrags Beschäftigten sowie etwaige Unterauftragsverarbeiter zur Geheimhaltung unter Berücksichtigung einschlägigen Rechts, insbesondere entsprechendem berufsständischen Recht.

5. Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

5.1. Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO, die mindestens die in **Anlage 3** spezifizierten Maßnahmen umfassen.

5.2. Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragsverarbeiter fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Die Angemessenheit der Maßnahmen sind regelmäßig durch den Auftragsverarbeiter zu überprüfen. Das Sicherheitsniveau der in **Anlage 3** festgelegten technischen und organisatorischen Maßnahmen darf nicht ohne schriftlich erteilte Zustimmung des Verantwortlichen unterschritten werden. Die schriftliche Zustimmung kann auch in einem elektronischen Format erfolgen.

5.3. Der Auftragsverarbeiter verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der **Anlage 3** schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Verantwortlichen zur Kenntnis zu geben.

6. Einsatz von Unterauftragsverarbeitern

6.1. Der Auftragsverarbeiter darf Unterauftragsverarbeiter in Anspruch nehmen, soweit diese, hinreichende Garantien im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen bieten. Etwaige zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen Unterauftragsverarbeiter sind aufgeführt in **Anlage 4** zu diesem Vertrag

Der Auftragsverarbeiter hat den Verantwortlichen schriftlich, was auch in einem elektronischen Format erfolgen kann, über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern zu informieren und stellt die erforderlichen Informationen zur Wahrnehmung des Einspruchsrechts im Rahmen oben genannter, aktualisierter Liste zur Verfügung. Gegen derartige Änderungen kann der Verantwortliche innerhalb einer Frist von 4 Wochen Einspruch erheben. Während der Laufzeit dieser Frist darf der Unterauftragsverarbeiter nicht hinzugezogen werden. Soweit der Verantwortliche Einspruch gegen die Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters erhebt, werden sich der Verantwortliche und der Auftragsverarbeiter innerhalb einer Frist von 4 Wochen untereinander abstimmen,

inwieweit die Einbeziehung des Unterauftragsverarbeiters nach Vorgaben des Verantwortlichen eingeschränkt oder ausgeschlossen werden kann oder der Vertrag – unter Berücksichtigung der einschlägigen Kündigungsfristen – zu beendigen ist.

6.2. Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Unterauftragsverarbeiter im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats im Wesentlichen dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Sofern ein Unterauftragsverarbeiter seine hieraus resultierenden Pflichten verletzt, informiert der Auftragsverarbeiter den Verantwortlichen entsprechend. Der Auftragsverarbeiter stellt sicher, dass jeder Unterauftragsverarbeiter die Verpflichtungen des Auftragsverarbeiters aus diesem Vertrag sowie der DSGVO erfüllt. Zudem muss der Verantwortliche berechtigt sein, Überprüfungen und Inspektionen, auch vor Ort, bei diesem Unterauftragsverarbeiter durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters.

6.3. Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters in Anspruch, so vereinbart er mit diesem eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – in die Rechte und Pflichten des nicht mehr bestehenden Auftragsverarbeiters aus dessen Vertrag zur Auftragsverarbeitung mit dem Unterauftragsverarbeiter eintritt und wahlweise das Recht hat, dieses Vertragsverhältnis zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7. Drittlandübermittlung

7.1. Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgt nur auf dokumentierte Weisung des Verantwortlichen und im Einklang mit Kapitel V der DSGVO.

7.2. Im Falle des Absatzes 1 kann der Auftragsverarbeiter mit jedem Unterauftragsverarbeiter die Standarddatenschutzklauseln der EU-Kommission (Modul „Processor to Processor“) gemäß Artikel 46 Abs. 2 DSGVO abschließen.

8. Mitwirkungs-/ Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen und berücksichtigt insoweit die Weisungen des Verantwortlichen. Soweit sich betroffene Personen zur Wahrnehmung ihrer Rechte an den Auftragsverarbeiter wenden, informiert dieser den Verantwortlichen unverzüglich. Insoweit sind die in **Anlage 2** aufgeführten Ansprechpartner zuständig. Der Auftragsverarbeiter antwortet auf eine Betroffenenanfrage erst nach Autorisierung des Verantwortlichen.

9. Unterstützung zur Pflichterfüllung des Verantwortlichen

9.1. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; Vorherige Konsultation) und gewährleistet insoweit die in **Anlage 3** beschriebenen technischen und organisatorischen Maßnahmen.

9.2. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich in Textform unter Berücksichtigung der Anforderungen gemäß Artikel 33 Absatz 3 und 4 DSGVO. Insoweit sind die in **Anlage 2** aufgeführten Ansprechpartner zuständig.

10. Löschung und Rückgabe personenbezogener Daten

10.1. Soweit gesetzliche oder anderweitige Aufbewahrungspflichten nicht entgegenstehen, wird der Auftragsverarbeiter – vorbehaltlich anderweitiger Weisungen des Verantwortlichen nach Ziffer 3 – bei Beendigung des Auftrags die verwendeten personenbezogenen Daten

☒ und die vorhandenen Kopien nach einem **schriftlichen** Hinweis an den Verantwortlichen und dem Ablauf einer Frist von 4 Wochen ab Eingang des Hinweises datenschutzkonform löschen.

10.2. Der Auftragsverarbeiter bestätigt gegenüber dem Verantwortlichen jede insoweit erfolgte Löschung in Textform. Stehen gesetzliche oder anderweitige Aufbewahrungspflichten einer Löschung oder Herausgabe entgegen, informiert der Auftragsverarbeiter den Verantwortlichen entsprechend in Textform.

10.3 Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieses Vertrages.

11. Pflichtennachweis und Unterstützung bei Überprüfungen

11.1. Die Parteien müssen in der Lage sein, die Einhaltung dieses Vertrages nachzuweisen.

11.2. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen und Dokumente zum Nachweis der Einhaltung der in Artikel 28 DSGVO und in diesem Vertrag niedergelegten Pflichten auf Anforderung zur Verfügung, einschließlich etwaiger Verträge mit Unterauftragsverarbeitern. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich

personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut etwaiger Verträge vor der Weitergabe einer Kopie unkenntlich machen.

11.3 Er ermöglicht Überprüfungen - einschließlich Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters ggf. mit angemessener Vorankündigung -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei. Die Festlegung der Art und Weise des Audits (z. B. remote oder vor Ort, per Fragebogen oder im persönlichen Interview) unterliegt der uneingeschränkten Entscheidungshoheit des Verantwortlichen. Der Verantwortliche kann seine Überprüfung nach eigenem Ermessen auch auf ein im Auftrag des Auftragsverarbeiters durchgeführtes Audit sowie auf einschlägige Zertifizierungen des Auftragsverarbeiters stützen.

11.4. Der Auftragsverarbeiter wird auftragsbezogene Anfragen des Verantwortlichen umgehend und in angemessener Weise beantworten.

11.5. Die Parteien stellen der zuständigen Aufsichtsbehörde auf Anfrage die Informationen, auf die sich die Ziffern 11.1-11.3 beziehen, zur Verfügung, wobei dies auch die Ergebnisse etwaiger Audits umfasst.

12. Sonstige Regelungen

12.1. Sollte die auftragsgemäße Erfüllung des Auftragsgegenstandes gemäß **Anlage 1** beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder ein Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Beteiligte unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Verantwortlichen liegen.

12.2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er nicht in der Lage ist, die Pflichten aus diesem Vertrag einzuhalten. Soweit der Auftragsverarbeiter Pflichten aus diesem Vertrag nicht erfüllt, kann der Verantwortliche den

Auftragsverarbeiter anweisen, die Verarbeitung auszusetzen, bis die vertragsgemäße Pflichterfüllung seitens des Auftragsverarbeiters gewährleistet ist. Soweit der Auftragsverarbeiter seine vertragsgemäße Pflichterfüllung oder die Einhaltung der DSGVO nicht innerhalb einer angemessenen Frist (spätestens innerhalb eines Monats) gewährleistet, kann der Verantwortliche den Vertrag außerordentlich kündigen. Das Recht zur außerordentlichen Kündigung des Verantwortlichen besteht darüber hinaus bei einem schwerwiegenden Pflichtverstoß des Auftragsverarbeiters gegen diesen Vertrag oder Pflichten nach der DSGVO. Gleiches gilt, wenn der Auftragsverarbeiter einer für ihn verbindlichen Entscheidung eines Gerichts oder der zuständigen Aufsichtsbehörde nicht nachkommt.

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

12.4. Jede Veränderung dieses Vertrages einschließlich seiner Kündigung und dieser Klausel bedarf der Schriftform, was auch in einem elektronischen Format erfolgen kann.

[**Ort**], den [**Datum**] Bonn, den

- *Auftragsverarbeiter* -	- DAAD als *Verantwortlicher* -

Anlage 1 des AV-Vertrags: Beschreibung der Verarbeitung

Gegenstand und Zweck der Verarbeitung

Der Gegenstand und Zweck der Verarbeitung ergibt sich aus dem schriftlichen Hauptvertrag

Rahmenvereinbarung zur Durchführung von Englischkursen im Vereinigten Königreich (UK) für Lehrende an deutschen Hochschulen,
Vergabe-Nr. 100/2026 vom [Datum des Zuschlags]

Dauer der Verarbeitung

Die Dauer der Verarbeitung ergibt sich aus dem schriftlichen Hauptvertrag.

Art der Verarbeitung

Die Verarbeitung der Daten erfolgt durch

☒ das Erheben

☒ das Erfassen

☒ das Aufnehmen

☒ die Organisation

☒ das Ordnen

☒ die Speicherung,

☐ die Archivierung,

☒ die Anpassung oder Veränderung

☒ das Auslesen

☒ das Abfragen

☒ die Verwendung

☒ die Offenlegung durch Übermittlung

☒ Verbreitung oder eine andere Form der Bereitstellung

☒ den Abgleich oder die Verknüpfung

☐ die Einschränkung

☒ das Löschen oder die Vernichtung

☐ sonstige Arten der Verarbeitung:

Kategorien personenbezogener Daten

Kategorien personenbezogener Daten, die Gegenstand der Verarbeitung sind:

☒ Adressdaten (Postanschrift)

☒ Abrechnungs- und Zahlungsdaten

☒ Namen

☐ Nutzerkennungen

☒ Alter

☐ Passwörter

☐ Arbeitszeitdaten

☐ Personenstammdaten

☒ Audiodaten

☒ Planungs- und Steuerungsdaten

☐ Bankverbindungsdaten

☐ Personal- und Identifikationsnummern

☒ Bewerberdaten

☒ Reisebuchungs- und -Abrechnungsdaten

☒ Bilddaten

☒ E-Mail-Adressen

☐ Telekommunikationsabrechnungsdaten

☐ Telekommunikationsverbindungsdaten

☒ Telefonnummern

☐ Hobbys

☐ Vertragsdaten

☐ Kreditkartendaten

☐ Kundenverhaltensdaten

☐ Kommunikationsdaten

☐ Kundenhistorie

☐ Lohn- und Gehaltsdaten

☐ Mitarbeiterbewertungen

☐ Mitarbeiterqualifikationen und -Eigenschaften

☒ Videodaten

☐ Zugangsdaten

☐ sonstige Kategorien personenbezogener Daten:

Kategorien sensibler personenbezogener Daten

Bearbeitungshinweis: Sensible Daten sind personenbezogene Daten, aus denen die rassische[3] oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten..

Kategorien sensibler personenbezogener Daten, die Gegenstand der Verarbeitung sind (sofern vorhanden):

☐ Gesundheitsdaten

☐ Religionszugehörigkeit

☐ Gewerkschaftszugehörigkeit

☐ politische Meinungen

☐ sonstige Kategorien sensibler personenbezogener Daten:

Angewandte Beschränkungen oder Garantien, die der Art der sensiblen personenbezogenen Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen:

☐ strenge Zweckbindung

☐ Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben)

☐ Aufzeichnungen über den Zugang zu den Daten

☐ Beschränkungen für Weiterübermittlungen

☐ zusätzliche Sicherheitsmaßnahmen **[…] Bitte ergänzen!**

☐ Sonstige Beschränkungen oder Garantien **[…] Bitte ergänzen!**

[3] Die Verwendung des Begriffs „rassische Herkunft“ entspricht dem Wortlaut der DSGVO. Die Verwendung dieses Begriffs in dieser Verordnung bedeutet nicht, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt (Erwägungsgrund zur DSGVO Nr. 51 S. 2).

Kategorien betroffener Personen

Im Wege der Auftragserfüllung verarbeitet der Auftragsverarbeiter personenbezogene Daten von folgenden Kategorien betroffener Personen:

☒ Beschäftigte	☒ Interessenten
☒ Auszubildende und Praktikanten	☐ Lieferanten und Dienstleister
☐ Bewerber	☒ Mieter
☐ ehemalige Arbeitnehmer	☒ Geschäftspartner
☐ freie Mitarbeiter	☐ Berater
☒ Vereinsmitglieder	☐ Besucher
☒ Geförderte	☐ Pressevertreter
☐ Alumni	☐ Abonnenten
☐ Angehörige von Beschäftigten	☐ Handelsvertreter
☐ Kunden	☐ Ansprechpartner

☐ sonstige Kategorien betroffener Personen:

Anlage 2 des AV-Vertrags: Ansprechpartner und Weisungen des Verantwortlichen

Bearbeitungshinweis: *Kontaktdaten der jeweiligen Ansprechpartner einschließlich Stellvertreter sollten ergänzt werden. Diesbezüglich wird empfohlen, personenunabhängige, funktionsbezogene Kontaktkanäle einzurichten (z. B. ds-verletzung@xyz.de, ds-betroffenenanfrage@xyz.de, ds-weisung@xyz.de).*

Anlass	**Rolle/Funktion des Ansprechpartners beim Verantwortlichen**	**Rolle/Funktion des Ansprechpartners beim Auftragsverarbeiter**
Weisungen	info@daad-akademie.de	
Betroffenenanfragen	datenschutz@daad.de	
Datenschutzverletzungen beim Auftragsverarbeiter	datenschutz@daad.de	
Inspektionen/Audits	datenschutz@daad.de	

Bearbeitungshinweis: *An dieser Stelle können optional bereits Weisungen des Verantwortlichen in diesen Vertrag aufgenommen werden. Insoweit kann für den Auftragsverarbeiter ein Ermessensspielraum bestehen bleiben, mit welchen geeigneten technischen und organisatorischen Maßnahmen die Weisungen umgesetzt werden.*

Kurzbezeichnung der Weisung	**Beschreibung der Weisung**

Anlage 3 des AV-Vertrags: Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Bearbeitungshinweis: *Diese Anlage 3 ist vom Auftragsverarbeiter auszufüllen. Sie spezifiziert die vom Auftragsverarbeiter ergriffenen technischen und organisatorischen Maßnahmen.*

Unter Berücksichtigung des

- Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs, der Umstände,
- der Zwecke der Verarbeitung,
- der Sensibilität der verarbeiteten personenbezogenen Daten, insbesondere im Hinblick auf besondere Kategorien personenbezogener Daten (s. Artikel 9 Abs. 1 DSGVO), sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Der Auftragsverarbeiter ergreift folgende Maßnahmen:

1. Maßnahmen zur Sicherstellung von Vertraulichkeit

Es ist zu gewährleisten, dass personenbezogene Daten ausschließlich von Befugten verarbeitet werden.

1.1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)

- ☐ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- ☐ Sicherheitstüren / -fenster
- ☐ Gitter vor Fenstern/Türen
- ☐ Zaunanlagen
- ☐ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☐ Werkschutz, Pförtner
- ☐ Alarmanlage
- ☐ Videoüberwachung
- ☐ Spezielle Schutzvorkehrungen des Serverraums
- ☐ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- ☐ Nicht-reversible Vernichtung von Datenträgern
- ☐ Mitarbeiter- und Berechtigungsausweise
- ☐ Sperrbereiche
- ☐ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

1.2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☐ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☐ Autorisierungsprozess für Zugangsberechtigungen
- ☐ Begrenzung der befugten Benutzer
- ☐ Single Sign-On
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Biometrischer Scan (Fingerabdruck, Iris, Gesicht)?
- ☐ BIOS-Passwörter
- ☐ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)

- ☐ Automatisierte Sperrung des Zugangs für bestimmten Zeitraum bei wiederholter Falscheingabe von Zugangsdaten?
- ☐ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- ☐ Personalisierte Chipkarten, Token, PIN-/TAN, etc.
- ☐ Protokollierung des Zugangs
- ☐ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☐ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☐ Firewall
- ☐ Systemspezifischer Schutz vor Angriffen / Intrusion Detection / Intrusion Prevention
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

1.3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☐ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☐ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☐ Autorisierungsprozess für Berechtigungen
- ☐ Genehmigungsroutinen
- ☐ Profile/Rollen
- ☐ Regelmäßige Kontrollen der Berechtigung von Zugriffsrechten gemäß „Need to know“
- ☐ Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem)

- ☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z. B. Kopierschutz, Sperrung von USB-Ports, „Data Loss Prevention (DLP)-System“)
- ☐ „Mobile Device Management-System“
- ☐ Vier-Augen-Prinzip
- ☐ Funktionstrennung „Segregation of Duties“
- ☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- ☐ Nicht-reversible Löschung von Datenträgern
- ☐ Protokollierung/Dokumentation von Löschungen
- ☐ Sichtschutzfolien für mobile Datenverarbeitungssysteme
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

1.4. Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken
- ☐ Getrennte Systeme
- ☐ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ☐ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ☐ Mandantenfähigkeit von IT-Systemen
- ☐ Verwendung von Testdaten
- ☐ Trennung von Entwicklungs- und Produktionsumgebung
- ☐ Sonstiges/ Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

2. Maßnahmen zur Verschlüsselung

Es ist zu gewährleisten, dass Zugang zum Klartext nur unter Verwendung eines (geheimen) Schlüssels möglich ist.

- ☐ Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones
- ☐ Verschlüsselung von mobilen Speichermedien (CD/DVD- ROM, USB-Stick, externen Festplatten)
- ☐ Verschlüsselung von Dateien

☐ Verschlüsselung von Systemen/Anlagen

☐ Verschlüsselte Aufbewahrung von Passwörtern

☐ Verschlüsselung von Email bzw.- Email-Anhängen

☐ Gesicherte Datenweitergabe (z. B. SSL, FTPS, TLS)

☐ Gesichertes WLAN

☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

3. Pseudonymisierung

Personenbezogene Daten werden in einer Weise verarbeitet, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Die Pseudonymisierung ist eine technische und organisatorische Maßnahme und kann vom Auftragsverarbeiter wie folgt umgesetzt werden:

☐ getrennte Speicherung von Zusatzinformationen zur Identifikation

☐ Verwendung von (Personal-, Kunden- oder Patienten-) Kennziffern statt Namen

☐ Verschlüsselung von Zusatzinformationen zur Identifikation

☐ Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation

☐ Autorisierungsprozess oder Genehmigungsroutinen für Berechtigungen zur Verarbeitung von Zusatzinformationen zur Identifikation

☐ Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation

☐ Vier-Augen-Prinzip für Identifikation

☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

4. Maßnahmen zur Sicherstellung von Integrität

Es ist zu gewährleisten, dass personenbezogene Daten korrekt und frei von Manipulationen verarbeitet werden.

☐ Zugriffsrechte

- ☐ Systemseitige Protokollierungen
- ☐ Dokumenten Management System (DMS) mit Änderungshistorie
- ☐ Sicherheits-/Protokollierungssoftware
- ☐ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☐ Mehraugenprinzip
- ☐ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)
- ☐ „Data Loss Prevention (DLP)-System“
- ☐ Elektronische Signatur
- ☐ Protokollierung von Datenübertragung oder Datentransport
- ☐ Protokollierung von lesenden Zugriffen
- ☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

5. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☐ Sicherheitskonzept für Software- und IT-Anwendungen
- ☐ Back-Up Verfahren
- ☐ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☐ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- ☐ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☐ Spiegeln von Festplatten
- ☐ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☐ Geeignete Archivierungsräumlichkeiten für Papierdokumente
- ☐ Brand- und/oder Löschwasserschutz des Serverraums
- ☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- ☐ Klimatisierter Serverraum
- ☐ Virenschutz
- ☐ Firewall
- ☐ Notfallplan

☐ Erfolgreiche Notfallübungen

☐ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

6. Maßnahmen zur Sicherstellung der Belastbarkeit

Es ist zu gewährleisten, dass die Datenverarbeitungssysteme hinreichend robust und widerstandsfähig sind, um die wichtigsten zu erwartenden Störungsereignisse zu bewältigen, ohne dass ihre Funktionsfähigkeit beeinträchtigt wird.

☐ Notfallplan für Maschinenausfall

☐ Redundante Stromversorgung

☐ Ausreichende Kapazität von IT-Systeme und Anlagen

☐ Logistisch gesteuerter Prozess zur Verhinderung von Leistungsspitzen

☐ Redundanten Systeme/Anlagen

☐ Resilienz und Fehler-Management

☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

7. Wirksamkeitskontrolle

Es ist zu gewährleisten, dass Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen existieren.

☐ Verfahren für regelmäßige Kontrollen/Audits

☐ Konzept für regelmäßige Überprüfung, Bewertung und Evaluierung

☐ Berichtswesen

☐ Penetrationstests

☐ Notfalltests

☐ Zertifizierung; falls vorhanden, [**Bitte ausführen**]

☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

8. Weisungskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden (auch bei einem Auftragsverarbeiter).

- ☐ Vertrag zur Auftragsdatenverarbeitung gem. Artikel 28 Abs. 3 DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen
- ☐ Richtlinien/Vorgaben zur Festlegung von datenschutzrechtlichen Verantwortlichkeiten/Zuständigkeiten
- ☐ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☐ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☐ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragsverarbeiter
- ☐ Unabhängige Auditierung der Weisungsgebundenheit
- ☐ Verpflichtung der Mitarbeiter zur Vertraulichkeit
- ☐ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- ☐ Benennung eines Datenschutzbeauftragten gemäß Artikel 37 ff. DSGVO
- ☐ Datenschutzmanager/-koordinator
- ☐ Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Artikel 30 Abs. 2 DSGVO
- ☐ Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten
- ☐ Richtlinien/Vorgaben zur Gewährleistung von technisch-organisatorischer Maßnahmen zur Sicherheit der Verarbeitung
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

9. Unterstützung des Verantwortlichen

Der Auftragsverarbeiter gewährleistet die erforderliche Unterstützung des Verantwortlichen bei dessen Pflicht

- *zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person,*
- *bei Meldungen von Datenschutzverletzungen an die zuständigen Aufsichtsbehörden und betroffenen Personen,*

- *zur Durchführung einer Datenschutz-Folgenabschätzung einschließlich einer etwaig erforderlichen Konsultation der zuständigen Aufsichtsbehörde und*
- *bei dessen Pflicht zur Gewährleistung der gebotenen Datenqualität (sachlich richtig und aktuell).*

☐ Richtlinien/Vorgaben zur Festlegung von datenschutzrechtlichen Verantwortlichkeiten/Zuständigkeiten

☐ Richtlinien/Vorgaben zur Gewährleistung von technisch-organisatorischer Maßnahmen zur Sicherheit der Verarbeitung

☐ Prozess zur Weiterleitung von Betroffenenanfragen

☐ Unterrichtung des Verantwortlichen bei Kenntnis von unrichtigen oder veralteten personenbezogenen Daten

☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO oder eines **genehmigten Zertifizierungsverfahrens** gemäß Artikel 42 DSGVO als Faktor zum Nachweis der Erfüllung der oben genannten Anforderungen (1. bis 8.):

☐ [**Bitte ausführen**]

Vorliegen anerkannter Zertifikate mit Bezug zu den oben genannten Anforderungen (z. B. ISO 27000-Reihe):

☐ [**Bitte ausführen**]

Anlage 4 des AV-Vertrags: Unterauftragsverarbeiter

Bearbeitungshinweis: *Diese Anlage 4 ist vom Auftragsverarbeiter auszufüllen.*

Name und Anschrift der Unterauftragsverarbeiter	Gegenstand, Art und Dauer der Unterbeauftragung	Erforderliche Informationen zur Entscheidung über Genehmigung/Einspruch durch Verantwortlichen, insbesondere Beschreibung des Nachweises angemessener technischer und organisatorischer Maßnahmen (z. B. Vertrag, dokumentiertes Konzept)
