

Vertrag zur Auftragsverarbeitung

gemäß Artikel 28 Datenschutz-Grundverordnung (DSGVO)¹

zwischen

Wissenschaftsrat – Geschäftsstelle des Wissenschaftsrates
Scheidtweilerstraße 4
50933 Köln

- Verantwortlicher² -

und

[Name und Anschrift des Auftragsverarbeiters]

- Auftragsverarbeiter -

nach Maßgabe der folgenden Bestimmungen:

[Passagen, die gelb markiert sind, werden im Zuge der Zuschlagserteilung ergänzt]

§ 1 Gegenstand und Dauer des Auftrags

1. Gegenstand des Auftrags

- ☒ Gegenstand des Auftrags ergibt sich aus dem zwischen Verantwortlichem und Auftragsverarbeiter geschlossenen Hauptvertrag und zwar dem **EVB-IT Cloudvertrag über die Bereitstellung einer DMS-Software in einer vom Auftragnehmer betriebenen Infrastruktur (SaaS) mit allen Anlagen vom [Datum]** (nachfolgend bezeichnet als „Hauptvertrag“).
- ☐ Gegenstand des Auftrags ergibt sich aus den Vergabeunterlagen inklusive Anlagen vom [Datum].
- ☐ Gegenstand des Auftrags ist: [Konkrete Beschreibung des Auftragsgegenstandes ergänzen]

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).

² Es gelten die Begriffsbestimmungen der DSGVO. In diesem Vertrag werden aus Gründen der besseren Lesbarkeit nach Möglichkeit genderneutrale Formulierungen gewählt. Falls dies nicht möglich ist, wird ausschließlich die männliche Form verwendet. Sie bezieht sich auf Personen ohne Berücksichtigung des Geschlechts.

2. Dauer des Auftrags

- ☒ Die Dauer des Auftrags ergibt sich aus dem Hauptvertrag.
- ☐ Der Auftrag beginnt mit Zuschlagserteilung am [Datum] und endet [Datum oder Ereignis].
- ☐ Der Auftrag beginnt mit Unterzeichnung dieses Vertrags und wird auf unbestimmte Zeit geschlossen. Er ist mit einer Frist von [Frist ergänzen] kündbar. Die Möglichkeit zur fristlosen Kündigung bei einem schwerwiegenden Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen des Vertrages bleibt hiervon unberührt.
- ☐ Der Auftrag wird zur einmaligen Ausführung in folgendem Zeitraum geschlossen: [konkreten Zeitraum ergänzen].

§ 2 Art und Zweck der Datenverwendung, Datenarten und Kategorien betroffener Personen, Rechte und Pflichten des Auftragsverarbeiters sowie des Verantwortlichen, Ort der Datenverarbeitung

1. Zweck der Datenverwendung

Die Tätigkeit des Auftragsverarbeiters dient

- ☐ den im Hauptvertrag vereinbarten Zwecken.
- ☐ den in den Vergabeunterlagen inklusive Anlagen vom [Datum] festgelegten Zwecken.
- ☒ den folgenden Zwecken: **Verwaltung der in der Organisation Wissenschaftsrat vorhandenen Dokumenten- und Datenbestände**

2. Art der Datenverwendung

Die Verwendung der Daten erfolgt durch folgende Datenverarbeitung im Auftrag des Verantwortlichen:

Im Zuge der Bereitstellung einer DMS-Software erfolgt eine Verarbeitung im Sinne des Art 4 Nr. 2 DSGVO durch mit Hilfe automatisierter Verfahren ausgeführte Vorgänge bzw. Vorgangsreihen im Zusammenhang mit personenbezogenen Daten wie insbesondere die Speicherung, die Anpassung oder Veränderung, die Organisation, das Ordnen, die Verwendung, die Offenlegung durch Übermittlung oder andere Formen der Bereitstellung, den Abgleich oder die Verknüpfung, das Löschen oder die Vernichtung.

3. Datenarten

- ☐ Datenarten, die Gegenstand dieses Auftrags sind, ergeben sich aus dem Hauptvertrag.
- ☒ Datenarten, die Gegenstand dieses Auftrags sind, ergeben sich aus **Anlage 1**.
- ☐ Datenarten, die Gegenstand dieses Auftrags sind, ergeben sich aus [sonstiges schriftliches Dokument ergänzen] vom [Datum].

4. Kategorien betroffener Personen

Im Wege der Auftragserfüllung verwendet der Auftragsverarbeiter personenbezogene Daten

- ☐ der im Hauptvertrag bestimmten Kategorien betroffener Personen.
- ☒ der in **Anlage 2** bestimmten Kategorien betroffener Personen.
- ☐ der in [sonstiges schriftliches Dokument ergänzen] vom [Datum] bestimmten Kategorien betroffener Personen.

5. Rechte und Pflichten des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter ist verpflichtet, sicherzustellen, dass er bzw. sein jeweiliger Unterauftragnehmer die auf Grundlage dieses Vertrages verarbeiteten personenbezogene Daten lediglich zum Zweck der Durchführung des Auftrags (siehe § 2 Absatz 1 dieses Vertrages) verarbeitet und diese nicht zu eigenen Zwecken weiterverarbeitet.
 - ☐ Zwischen dem Verantwortlichen und dem Auftragsverarbeiter wird abweichend von der vorstehenden Regelung vereinbart, dass der Auftragsverarbeiter berechtigt ist, Daten des Verantwortlichen zu eigenen Zwecken weiterzuverarbeiten (z. B. zur Weiterentwicklung und Fehleranalyse der Systeme). Insoweit werden Zwecke und Maßnahmen der Verarbeitung im Folgenden abschließend definiert und festgelegt:
 - Zweck der Weiterverarbeitung durch den Auftragsverarbeiter: [\[Zweck der Weiterverarbeitung ergänzen\]](#).
 - Maßnahmen, die vom Auftragsverarbeiter ergriffen werden, um das mit der Verarbeitung verbundene Risiko zu minimieren (z. B. Anonymisierung): [\[Maßnahmen zur Risikominimierung ergänzen\]](#).
- (2) Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher Zustimmung in Textform durch den Verantwortlichen erteilen, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet. Insoweit sind die in **Anlage 4** aufgeführten Ansprechpartner zuständig.
- (3) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.
- (4) Der Auftragsverarbeiter gewährleistet, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen Zustimmung des Verantwortlichen in Textform, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

6. 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 sie anwendbaren und verbindlichen Datenschutzrechts der

Mitgliedstaaten sowie die Wahrung der Rechte der betroffenen Personen nach den Artikeln 7, 12 bis 22 DSGVO verantwortlich.

- ☐ Die Parteien vereinbaren zusätzlich folgende Rechte und Pflichten des Verantwortlichen: [Klicken oder tippen Sie hier, um Text einzugeben.](#)

7. Orte der Datenverarbeitung

Die Orte der Datenverarbeitung beim Auftragsverarbeiter werden in **Anlage 3** zu diesem Vertrag vertraglich festgelegt.

§ 3 Weisungsgebundene Verarbeitung und Remonstrationspflicht

- (5) Für Weisungen des Verantwortlichen gegenüber dem Auftragsverarbeiter (Artikel 29 i. V. m. Artikel 28 Absatz 3 Buchstabe a DSGVO) sind die in **Anlage 4** aufgeführten Ansprechpersonen zuständig. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf in Textform dokumentierte Weisung des Verantwortlichen auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation 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 in Textform vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Darüber hinaus erfolgt die Verarbeitung durch den Auftragsverarbeiter gemäß etwaiger in **Anlage 4** festgelegter Weisungen.
- (6) Weisungen werden vom Verantwortlichen grundsätzlich in Textform (z. B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom
- ☒ Verantwortlichen
 - ☒ Auftragsverarbeiter
- entsprechend in Textform (z. B. per E-Mail) bestätigt.
- (7) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich in Textform 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).

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

- (1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung. Der Auftragsverarbeiter stellt sicher, dass diese Personen nur im Rahmen der Erforderlichkeit auf personenbezogene Daten der beauftragten Verarbeitungstätigkeit zugreifen („Need to know“).
- (2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze

ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

- (3) Sofern der Auftragsverarbeiter der gesetzlichen Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragte/n unterliegt, sind die Kontaktdaten der/des Datenschutzbeauftragten dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen. Unterliegt der Auftragsverarbeiter nicht der Benennungspflicht, teilt er dem Verantwortlichen die Kontaktdaten eines Ansprechpartners für den Datenschutz mit.
- (4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

- (1) Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO. Die Vertragsparteien vereinbaren die in **Anlage 5** zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen.
- (2) Ergibt eine Prüfung des Verantwortlichen einen Anpassungsbedarf der vom Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen gemäß Artikel 32 DSGVO, sind die Anpassungen vom Auftragsverarbeiter umzusetzen.
- (3) 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. Das Sicherheitsniveau der in **Anlage 5** festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.
- (4) Der Auftragsverarbeiter verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der **Anlage 5** in Textform zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Verantwortlichen zur Kenntnis zugeben.

§ 6 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

- (1) Der Auftragsverarbeiter (auch erster Auftragsverarbeiter) nimmt keine weiteren Auftragsverarbeiter ohne vorherige Zustimmung des Verantwortlichen in Textform in Anspruch. Etwaige zum Zeitpunkt des Vertragsschlusses mit Zustimmung des Verantwortlichen in Anspruch genommenen weiteren Auftragsverarbeiter sind in **Anlage 6** zu diesem Vertrag aufgeführt.

- (2) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters (Unterauftragnehmer) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesen weiteren Auftragsverarbeiter 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 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. Der Auftragsverarbeiter stellt weiterhin sicher, dass die weiteren Auftragsverarbeiter den Nachweis der DSGVO-Konformität erbringen (z. B. durch eine aktuelle Datenschutz-Zertifizierung durch eine nach der Norm der ISO/IEC 17065 akkreditierte Stelle oder durch ein Audit einer sonstigen unabhängigen Stelle).
- (3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem/den weiteren Auftragsverarbeiter/n Kontroll- und Überprüfungsrechte entsprechend der hiesigen Vereinbarung einzuräumen. Demnach ist der Verantwortliche berechtigt, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei diesem/diesen weiteren Auftragsverarbeiter/n durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Ebenso ist der Verantwortliche berechtigt, auf in Textform erfolgte Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem/den weiteren Auftragsverarbeiter/n geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des/der weiteren Auftragsverarbeiter/s zu erhalten.
- (4) Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung dieses/dieser weiteren Auftragsverarbeiter/s ganz oder teilweise zu beenden oder das Vertragsverhältnis mit diesem/diesen weiteren Auftragsverarbeiter/n zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.
- (5) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, so vereinbart er darüber hinaus mit diesem eine Drittbegünstigtenklausel, nach der der Verantwortliche im Fall einer Insolvenz des Auftragsverarbeiters befugt ist, seine Rechte aus diesem Vertrag unmittelbar gegenüber dem weiteren Auftragsverarbeiter durchzusetzen, etwa das Recht, die Vernichtung oder die Rückgabe der personenbezogenen Daten anzuweisen.

§ 7 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 4** aufgeführten Ansprechpartner zuständig.

§ 8 Unterstützung zur Pflichterfüllung des Verantwortlichen

- (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).
- (2) Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen, insbesondere bei einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO.

Insoweit sind die in **Anlage 4** aufgeführten Ansprechpartner zuständig.

Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieser Vereinbarung durchführen.

§ 9 Löschung und Rückgabe personenbezogener Daten

Soweit gesetzliche oder anderweitige Aufbewahrungspflichten nicht entgegenstehen, wird der Auftragsverarbeiter nach Beendigung des Auftrags die verwendeten personenbezogenen Daten

- ☐ und die vorhandenen Kopien unverzüglich datenschutzkonform löschen.
- ☒ dem Verantwortlichen in einer für den Verantwortlichen lesbaren und bearbeitbaren Form herausgeben und die vorhandenen Kopien datenschutzkonform löschen, soweit der Verantwortliche ihn nicht in Textform anweist, die personenbezogenen Daten und die vorhandenen Kopien datenschutzkonform zu löschen. Der Auftragsverarbeiter stimmt im Falle der Herausgabe der Daten das Format mit dem Verantwortlichen ab, um die Nutzbarkeit sicherzustellen.
- ☐ und die vorhandenen Kopien nach einem [optional: schriftlichen] Hinweis an den Verantwortlichen und dem Ablauf einer Frist von [Angabe einer Frist] ab Eingang des Hinweises datenschutzkonform löschen.
- ☐ und die vorhandenen Kopien nach Genehmigung durch den Verantwortlichen datenschutzkonform löschen.

§ 10 Pflichtennachweis und Unterstützung bei Überprüfungen

- (1) 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 weiteren Auftragsverarbeitern. Er ermöglicht Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei.
- (2) Die Überprüfung kann auch auf der Grundlage vorgelegter aktueller Testate, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 DSGVO und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.
- (3) Die Überprüfung kann auch durch eine Inspektion vor Ort erfolgen. Der Verantwortliche kann sich hierzu in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieser Vereinbarung erforderlichen technischen und organisatorischen Erfordernisse überzeugen.
- (4) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 1 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.
- (5) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 11 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen zur Erfüllung ihrer bzw. seiner jeweiligen gesetzlich zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiterinnen und Mitarbeiter anweisen, mit dem/ der Datenschutzbeauftragten zu kooperieren, insbesondere ihre bzw. seine Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 12 Sonstige Regelungen

- (1) Sollte die auftragsgemäße Erfüllung des Auftragsgegenstandes gemäß § 1 dieses Vertrages 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.
- (2) Die Parteien sind sich einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter
- (3) Bei etwaigen Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags den Regelungen des Hauptvertrags vor.
- (4) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.
- (5) Soweit in dieser Vereinbarung von Textform die Rede ist, ist die Textform gemäß § 126b BGB gemeint.
- (6) Jede Veränderung dieses Vertrages einschließlich seiner Kündigung und dieser Klausel bedarf der Schriftform, was auch in einem elektronischen Format erfolgen kann.

§ 12 Inkrafttreten

Dieser Vertrag wird mit Zuschlagserteilung wirksam.

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Datum, Name

Datum, Name

Anlagen:

Anlage 1	Datenarten
Anlage 2	Kategorien betroffener Personen
Anlage 3	Orte der Datenverarbeitung
Anlage 4	Ansprechpartner und Weisungen des Verantwortlichen
Anlage 5	Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO
Anlage 6	Weitere Auftragsverarbeiter

Anlage 1

Datenarten

Folgende Datenarten sind Gegenstand dieses Auftrags:

- | | |
|---|--|
| ☒ Adressdaten | ☒ Namen |
| ☒ Abrechnungs- und Zahlungsdaten | ☒ Nutzerkennungen |
| ☒ Alter | ☐ Passwörter |
| ☒ Arbeitszeitdaten | ☒ Personenstammdaten |
| ☒ Audiodaten | ☐ Planungs- und Steuerungsdaten |
| ☒ Bankverbindungsdaten | ☒ Personal- und Identifikationsnummern |
| ☒ Bewerberdaten | ☒ Reisebuchungs- / –Abrechnungsdaten |
| ☒ Bilddaten | ☒ Telekommunikationsabrechnungsdaten |
| ☒ E-Mails | ☒ Telekommunikationsverbindungsdaten |
| ☒ Gesundheitsdaten | ☒ Telefonnummern |
| ☐ Hobbys | ☒ Vertragsdaten |
| ☒ Kreditkartendaten | ☒ Videodaten |
| ☐ Kundenverhaltensdaten | ☐ Zugangsdaten |
| ☒ Kommunikationsdaten | ☐ Sonstige: [Bitte ausführen] |
| ☒ Kundenhistorie | |
| ☒ Lohn- und Gehaltsdaten | |
| ☒ Mitarbeiterbewertungen | |
| ☒ Mitarbeiterqualifikationen und –Eigenschaften | |

Anlage 2

Kategorien betroffener Personen

Folgende Kategorien betroffener Personen sind Gegenstand des Auftrags:

- ☒ Beschäftigte
- ☒ Auszubildende und Praktikanten
- ☒ Bewerber
- ☒ ehemalige Arbeitnehmer
- ☒ freie Mitarbeiter
- ☐ Gesellschafter
- ☒ Angehörige von Beschäftigten
- ☐ Antragstellende
- ☒ Gutachtende
- ☒ Gremienmitglieder
- ☐ Kunden
- ☐ Interessenten
- ☒ Lieferanten und Dienstleister
- ☐ Mieter
- ☒ Geschäftspartner
- ☒ Berater
- ☐ Besucher
- ☒ Pressevertreter
- ☐ Abonnenten
- ☐ Handelsvertreter
- ☒ Ansprechpartner
- ☐ Sonstige: [Bitte ausführen]

Anlage 3

Orte der Datenverarbeitung beim Auftragsverarbeiter

Der Auftragsverarbeiter stellt die Datenverarbeitung an folgenden Orten sicher:

Ort der Datenverarbeitung (Serverstandort/e)	Gegenstand und Zweck der Datenverarbeitung
Serverstandorte	[wird ergänzt gemäß Angebot]

Anlage 4
Ansprechpartner und Weisungen des Verantwortlichen

Anlass	Rolle/Funktion des Ansprechpartners beim Verantwortlichen³	Rolle/Funktion des Ansprechpartners beim Auftragsverarbeiter
Weisung	[Name 1] Tel. [Telefonnummer] E-Mail: [E-Mail-Adresse] [Funktion] [ggf. Name 2] Tel. [Telefonnummer] E-Mail: [E-Mail-Adresse] [Funktion]	[Name 1] Tel. [Telefonnummer] E-Mail: [E-Mail-Adresse] Unternehmen: [Unternehmenszugehörigkeit] [Funktion] [ggf. Name 2] Tel. [Telefonnummer] Unternehmen: [Unternehmenszugehörigkeit] E-Mail: [E-Mail-Adresse] [Funktion]
Betroffenenanfrage	Ansprechpartner zum Datenschutzmanagement: [Name 1] Tel: [Telefonnummer] E-Mail: datenschutz@wissenschaftsrat.de	[Name 1] Tel. [Telefonnummer] Unternehmen: [Unternehmenszugehörigkeit] E-Mail: [E-Mail-Adresse] [Funktion] [ggf. Name 2] Tel. [Telefonnummer] Unternehmen: [Unternehmenszugehörigkeit] E-Mail: [E-Mail-Adresse] [Funktion]
Datenschutzverletzung beim Auftragsverarbeiter	Ansprechpartner zum Datenschutzmanagement: [Name 1] Tel: [Telefonnummer] E-Mail: datenschutz@wissenschaftsrat.de	[Name 1] Tel. [Telefonnummer] E-Mail: [E-Mail-Adresse] Unternehmen: [Unternehmenszugehörigkeit] [Funktion] [ggf. Name 2] Tel. [Telefonnummer] E-Mail: [E-Mail-Adresse] Unternehmen: [Unternehmenszugehörigkeit] [Funktion]

³ gilt für die Zeit der Federführung des Wissenschaftsrates

Kurzbezeichnung der Weisung	Beschreibung der Weisung
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.	Klicken oder tippen Sie hier, um Text einzugeben.

[wird im Falle von Weisungen genutzt]

Anlage 5

Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Unter Berücksichtigung des

- Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und
- der Zwecke der Verarbeitung 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:

[wird im Zuge der Zuschlagserteilung gemäß Angebot ergänzt]

1. Maßnahmen zur Sicherstellung von Vertraulichkeit

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

a. Zutrittskontrolle

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

- ☐ Zutrittskontrollsystem: Ausweisleser, Magnetkarte, Chipkarte
- ☐ Schlüssel / Schlüsselvergabe
- ☐ Türsicherung (elektrische Türöffner usw.)
- ☐ Gebäudesicherung (Zäune, Pforten)
- ☐ Werkschutz, Pförtner
- ☐ Überwachungseinrichtung: Alarmanlage, Video- / Fernsehmonitor
- ☐ Biometrisches Zugangssystem
- ☐ Alarmsicherung
- ☐ Tragepflicht von Ausweisen / Ausweissystem
- ☐ Absicherung von Gebäudeschächten

- ☐ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
- ☐ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen
- ☐ Schließsystem
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

b. Zugangskontrolle

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

- ☐ Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- ☐ Two-Factor Authentication
- ☐ Intrusion Detection Systeme
- ☐ Intrusion Prevention Systeme
- ☐ Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- ☐ Einrichtung eines Benutzerstammsatzes pro User
- ☐ Software Firewall
- ☐ Hardware Firewall
- ☐ Einsatz von zentraler Administrations-Software für mobile Endgeräte (z.B. zum externen Sperren und Löschen von Daten)
- ☐ BIOS-Schutz
- ☐ Allgemeine Richtlinie Datenschutz/Datensicherheit verabschiedet
- ☐ Richtlinie zum Ausscheiden von Mitarbeitern existiert (Rechteentzug)
- ☐ Passwortrichtlinie verabschiedet
- ☐ Gehäuseschutz
- ☐ Schutzmaßnahmen zur Sicherung bei Nutzung von eigenen Geräten durch Mitarbeiter (z.B. Fernlöschung oder -sperrung)
- ☐ Anti-Viren Software
- ☐ Autorisierungsprozess für Zugangsberechtigungen
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

c. 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.

- ☐ Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte, Prinzip "Need to know")
- ☐ Benutzererkennung mit Passwort
- ☐ Ausgabe von Zertifikaten zur Authentifizierung

- ☐ Sicherung von Schnittstellen (USB, Firewire usw.)
- ☐ Virenschutz / Firewall
- ☐ Regelmäßige Updates der Systeme
- ☐ Klassische Rollen(Auswertungen, Kenntnisnahme, Veränderung, Löschung)
- ☐ Protokollierung von Zugriffen in Logs
- ☐ Verschlüsselung von Datenträgern
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

d. Trennungskontrolle

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

- ☐ "Interne Mandantenfähigkeit"
- ☐ Zweckbindung
- ☐ Separierung Datenbanken
- ☐ Separierung von Tables in Datenbanken
- ☐ Funktionstrennung / Produktion / Test & Sandboxing
- ☐ Sonstiges/ Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

2. Pseudonymisierung

Personenbezogene Daten können in einer Weise verarbeitet werden, so dass sie 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 eine unbefugte Identifizierung der Betroffenen gewährleisten. Die Pseudonymisierung ist eine technische und organisatorische Maßnahme und kann vom Auftragsverarbeiter wie folgt umgesetzt werden:

- ☐ Umwandeln von Identifikationsmerkmalen in zufällige Zeichenfolgen (z.B. Namen und Geburtsdaten)
- ☐ Identifizierung von Datensätzen mit IDs anstatt Klarnamen und anderen persönlichen Daten
- ☐ Keine Eingabemöglichkeiten von nicht pseudonymen Daten (z.B. Angabe von Nicknames statt Klarnamen)
- ☐ Kontrolle der Bestimmbarkeit bei Kumulation von Datensätzen
- ☐ Automatische Pseudonymisierungsverfahren bei neuen Datensätzen
- ☐ Aufhebung der Pseudonymisierung nur im Vier-Augen-Prinzip
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

3. Maßnahmen zur Sicherstellung von Integrität

Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

- ☐ Verschlüsselung / Tunnelverbindung
- ☐ Prüfung der Rechtmäßigkeit der Weitergabe von Daten

- ☐ Regelungen zum datenschutzkonformen Vernichten von Datenträgern
- ☐ Verfahrensverzeichnis
- ☐ Elektronische Signatur
- ☐ E-Mail Verschlüsselung
- ☐ Protokollierung
- ☐ Transportsicherung
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

- ☐ Dokumentenmanagement, Dokumentenlenkung
- ☐ Protokollierungs- und Protokollauswertungssysteme (3 Monate Revisionssicher)
- ☐ Plausibilitätskontrollen
- ☐ Löschkonzept und klare Zuständigkeiten für die Löschung
- ☐ Sicherung von Protokolldaten gegen Verlust oder Veränderung
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

4. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust).

- ☐ Backup-Strategie (offline)
- ☐ Backup-Strategie (online, z.B. Cloud)
- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Datenschutztresore
- ☐ Analyse der Serverraumlage (z.B. Sanitärleitungen)
- ☐ Löschanlagen
- ☐ Videoüberwachung im Serverraum
- ☐ Getrennte Aufbewahrung
- ☐ Überspannungsschutz
- ☐ Schutz vor Diebstahl
- ☐ Virenschutz / Firewall
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen).

- ☐ Notfallmanagement inkl. Notfallpläne
- ☐ Testen der Wiederherstellungssysteme
- ☐ Incident Management

- ☐ Zertifizierung (z.B.: ISO-Zertifizierung)
- ☐ Penetrationstests
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

5. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- ☐ Datenschutz-Management System etabliert
- ☐ Regelmäßige Datenschutzbildungen
- ☐ Incident-Response-Management
- ☐ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- ☐ Auftragskontrolle (BCR, einheitliche Vertragsbedingungen)
- ☐ Auftragskontrolle (AV)
- ☐ Eindeutige Vertragsgestaltung
- ☐ Sicherheitszertifizierung (z.B. ISO)
- ☐ Prozesse und Verantwortlichkeiten für Sicherheitsvorfälle
- ☐ Überprüfung der TOM in regelmäßigem Turnus (z.B. 1x jährlich)
- ☐ Regelmäßige und umfangreiche Datenschutzbildungen
- ☐ Benennung eines Informationssicherheitsbeauftragten
- ☐ Vorabüberzeugungspflicht
- ☐ Nachkontrollen
- ☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [Bitte ausführen]

6. **Technische und organisatorische Umsetzung des Rechts auf Löschung, "Recht auf Vergessenwerden"**

Folgende Maßnahmen wurden ergriffen:

- ☐ Einfache Datenlöschung (ohne Überschreiben)
- ☐ Randomisiertes Überschreiben von Datensätzen
- ☐ Implementierung von Fernlöschung, z.B. auf mobilen Endgeräten
- ☐ Zerstörung von Datenträgern vor der Entsorgung
- ☐ Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern
- ☐ Entmagnetisierung von physischen Datenträgern (Festplatten / Datenbändern)
- ☐ Automatische Löschung von Datensätzen nach einem festgelegten Ablaufdatum
- ☐ Richtlinien zur Vernichtung von Daten nach Beendigung eines Vertragsverhältnisses
- ☐ Sorgfältige Auswahl von Entsorgungsdienstleistern
- ☐ Klassifikation der Daten in Schutzklassen

- ☐ Umsetzung der DIN-EN 15713 "Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln"
- ☐ Protokollierung von Löschvorgängen
- ☐ 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 6.):

- ☐ [Bitte ausführen]

Anlage 6

Weitere Auftragsverarbeiter

[wird im Zuge der Zuschlagserteilung gemäß Angebot ergänzt]

Name und Anschrift der weiteren Auftragsverarbeiter	Gegenstand und Zweck der Unterbeauftragung	Ort der Datenverarbeitung (Serverstandort/e)
Weitere Auftragsverarbeiter 1	Gegenstand	Serverstandort/e
Weitere Auftragsverarbeiter 2	Gegenstand	Serverstandort/e