

Vereinbarung zur Auftragsverarbeitung

Goethe-Institut e.V.
Oskar-von-Miller-Ring 18
80333 München

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

und

Auftragnehmer ergänzen

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

beide zusammen nachstehend „**Parteien**“ 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: „**Services**“) beauftragt. Die vorliegende Vereinbarung („**AV-Vereinbarung**“) ergänzt den Vertrag um Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO.
- 1.2 Soweit der AN im Rahmen der Leistungserbringung (1) personenbezogene Daten, für die der AG datenschutzrechtlich Verantwortlicher ist, (kurz: „**Daten**“) verarbeitet und/oder (2) die Möglichkeit des Zugriffs auf personenbezogene Daten erhält, 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 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.
- 1.5 Beginn, Dauer, Ende und Kündigungsmöglichkeiten der AV-Vereinbarung entsprechen denjenigen des Vertrags. Das Recht zur außerordentlichen Kündigung dieser AV-Vereinbarung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, 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. 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** festgelegt.
- 2.2 Der AN verarbeitet die Daten ausschließlich im Rahmen dieser AV-Vereinbarung, insbesondere nach den relevanten Vorgaben der **Anlage 1**, sowie etwaiger dokumentierter Einzelweisungen des AG nach Ziffer 2.3.

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 mindestens in Textform mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Mit Ausnahme vorstehender 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 mindestens in Textform zu erteilen. Bei Gefahr in Verzug kann der AG eine Einzelweisung auch mündlich erteilen. Der AG hat diese im Anschluss unverzüglich mindestens in Textform 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 so lange 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 zustehender 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. Der AN unterstützt den AG bei der Beantwortung der Betroffenenanfragen, sofern der AG nicht über die dafür erforderlichen Informationen verfügt.
- 2.6. Der AN ist verpflichtet, Zugang und Zugriff auf die Daten streng auf die Personen zu begrenzen, die zur Erbringung der Services auf die Daten zugreifen müssen. Der AN ist ferner verpflichtet, die bei der Durchführung der Arbeiten beschäftigten Personen vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut zu machen und für die Zeit ihrer Tätigkeit wie auch im Anschluss in geeigneter Weise auf die Einhaltung des Datenschutzes zu verpflichten.
- 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 mindestens in Textform nach und legt deren Dokumentation vor. Der AN hat alle Verarbeitungstätigkeiten, die er im Rahmen der AV-Vereinbarung für den AG durchführt, gemäß Art. 30 Abs. 2 DSGVO zu dokumentieren. Auf Anforderung des AG stellt der AN dem AG diese Dokumentation zur Verfügung.
- 2.8 Der AN erstattet dem AG unverzüglich schriftlich oder in Textform und unter Angabe von Details Meldung bei den folgenden **Datenschutzvorkommnissen**:
 - (1) Verdacht auf Verletzungen des Schutzes personenbezogener Daten,
 - (2) Verstößen 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,
 - (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 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 zu machen und Fragen des AG zu 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 oder Abweichung, 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 oder Abweichung; und
- (3) eine Beschreibung der vom AN ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder Abweichung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

2.10 Informationen zum betrieblichen Datenschutzbeauftragten („DSB“) des AN sowie weitere Angaben des AN zu seiner Datenschutz-Organisation sind in **Anlage 2** festgelegt und durch den Auftragnehmer zugesichert. Ein Wechsel des DSB oder sonstige Änderungen der Angaben in **Anlage 2** hat der AN dem AG unverzüglich in Schrift- oder Textform mitzuteilen.

2.11 Der AN unterstützt den AG mit geeigneten technischen und organisatorischen Maßnahmen, den Betroffenenrechten 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 gesetzlicher Vorgaben benötigt (etwa zur Erstellung des Verzeichnisses von Verarbeitungstätigkeiten).

2.12 Der AN hat die Daten von sonstigen Datenbeständen (eigene des AN oder von anderen Kunden des AN) strikt zu trennen; 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 Mitgliedsstaaten der Europäischen Union (EU), anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) oder in Ländern, für die ein Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO vorliegt (**„Länder mit angemessenem Datenschutzniveau“**); 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.) die Daten nicht in dem in Ziffer 3.1 genannten Gebiet 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 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 des in Ziffer 3.1. genannten Gebiets 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, mobilem Arbeiten, o.Ä.) ist nur mit Zustimmung des AG zulässig. Die Zustimmung setzt voraus, dass (1) auch am Ort der Datenverarbeitung diejenigen technischen und organisatorischen Maßnahmen gelten, wie in der Anlage 5 zu dieser AVV vereinbart, und (2) 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 Vereinbarung inkl. deren Anlagen sorgt. Dies hat der AN mit seinen Mitarbeitern vertraglich sicherzustellen, indem er mindestens folgende Inhalte regelt:

- Home-Office ist ausschließlich mit den hierfür vom Arbeitgeber bereitgestellten Mitteln (u.a. Hardware, Anwendungen, Verbindungsmöglichkeiten) erlaubt.
- Es ist ausschließlich die Nutzung durch die IT-Abteilung vorinstallierter oder durch diese im Einzelfall freigegebener Anwendungen zulässig. Dies gilt ausdrücklich auch für portable Software oder Betriebssysteme von Wechseldatenträgern.
- Die lokalen Laufwerke eines Computers sind für den Start von Anwendungen und den Betrieb während des Arbeitstages gedacht. Lokal verarbeitete Daten sind auch im Home-Office spätestens am Ende des Arbeitstages entsprechend zu sichern, z.B. auf durch Ablage auf serverbasierenden Laufwerken. Eine Ausnahme besteht nur dann, wenn die Verbindung zu den serverbasierenden Laufwerken o.ä. vorübergehend nicht gegeben ist. In diesem Falle ist die Sicherung bei nächstmöglicher Gelegenheit nachzuholen.
- Ausdrucke, die personenbezogene Daten beinhalten, dürfen im Home-Office nur erfolgen, wenn sichergestellt ist, dass diese sicher vernichtet werden können.
- Home-Office darf auch innerhalb der eigenen Wohnräume ausschließlich an Orten und unter solchen Umständen erfolgen, welche die Vertraulichkeit, Integrität und Verfügbarkeit gewährleisten. Insbesondere darf Dritten zu keiner Zeit eine Kenntnisnahme der verarbeiteten Daten möglich sein. Dritte sind auch Personen, welche sich im gleichen Haushalt wie der Arbeitnehmer aufhalten.
- Eingesetzte Geräte und Informationen müssen auch innerhalb der Wohnräume jederzeit sicher transportiert und beaufsichtigt werden. Notebooks, USB-Sticks etc. müssen den Mitarbeitern vom Auftragnehmer verschlüsselt zur Verfügung gestellt werden.
- Bei kurzzeitiger Abwesenheit sind genutzte Geräte zu sperren (z.B. Bildschirm Sperre) und Informationen wirksam gegen unbefugten Zugriff zu sichern (z.B. Passwort). Bei längerer Abwesenheit sind sämtliche Informationen und Arbeitsmittel sicher zu verwahren und nach Möglichkeit einzuschließen

Soweit für die Verarbeitung personenbezogener Daten des AG für das Homeoffice eines Mitarbeiters des AN Abweichungen zu den in der **Anlage 5** zu dieser AV-Vereinbarung vereinbarten technischen und organisatorischen Maßnahmen gelten, müssen diese vom AN gesondert ausgewiesen und vom AG akzeptiert sein.

4. Einschaltung von Unterauftragnehmern

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

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

Setzt der AN nach Abschluss dieser AV-Vereinbarung weitere Unterauftragnehmer ein, gilt die Zustimmung des AG im Sinne der Ziffer 4.1 als erteilt, wenn der AN dem AG unverzüglich eine aktualisierte Fassung der **Anlage 4** vorlegt und der AG nicht innerhalb von 4 Wochen nach Erhalt der neuen Fassung der **Anlage 4** widerspricht.

4.3 Soweit der AN mit entsprechender Zustimmung des AG Unterauftragnehmer einschaltet, die die Datenverarbeitung außerhalb des in Ziffer 3.1 genannten Gebiets vornehmen, muss der AN dabei zwingend die Voraussetzungen der Art. 44 bis 49 DSGVO einhalten und dies dem AG nachweisen.

4.4 Der AN hat in jedem Fall seine Verträge mit Unterauftragnehmern so zu gestalten, dass sie datenschutzrechtlich mindestens den Datenschutzbestimmungen der 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. Der Vertrag 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 den einschlägigen Datenschutzgesetzen erfolgt.

4.5 Der AN ist im Verhältnis zum AG für die bestmögliche und datenschutzkonforme Auswahl von geeigneten Unterauftragnehmern sowie die 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 und 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 Unterauftragnehmern 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 ein für dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau. Dazu berücksichtigt der AN die Schutzziele von Art. 32 DSGVO derart, dass durch geeignete technische und organisatorische Maßnahmen das Risiko auf Dauer möglichst ausgeschlossen wird.
- 5.2 Das in **Anlage 5** beschriebene Datensicherheitskonzept legt die Auswahl der technischen und organisatorischen Maßnahmen (kurz: „**TOMs**“) passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim AN fest. Der AN ist verpflichtet, die TOMs 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 TOMs anzupassen, soweit es sich um adäquate Maßnahmen handelt und zugleich das Sicherheitsniveau der in **Anlage 5** festgelegten TOMs nicht unterschritten wird. Auf Aufforderung des AG informiert der AN den AG über solche Änderungen, wesentliche Änderungen sind dagegen vor ihrer Einführung einvernehmlich festzulegen.
- 5.4 Die Parteien sind sich einig, dass die Bestimmungen der **Anlage 5** für die Verarbeitung von Informationen entsprechend gelten, die nicht personenbezogen sind, aber aus anderen Gründen schützenswert sind (kurz „**schützenswerte Informationen**“), Schützenswerte Informationen im Sinne dieser AVV sind alle Informationen, die vom AG ausdrücklich als vertraulich gekennzeichnet wurden oder deren Vertraulichkeit sich aus den Umständen der Offenlegung gegenüber dem AN oder der Information selbst ergibt.

6. Kontrollen des AG

- 6.1 Der AG ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz, dieser AV-Vereinbarung samt ihrer Anlagen, insbesondere auch der vereinbarten TOMs nach **Anlage 5**, selbst oder durch Dritte zu kontrollieren, insbesondere durch Einholung von Auskünften und die Einsichtnahme in gespeicherte Daten und die Datenverarbeitungsprogramme sowie mit angemessener Vorankündigung auch durch Kontrollen beim AN vor Ort. Begründen tatsächliche Anhaltspunkte den Verdacht, es habe sich ein Datenschutzvorkommnis i.S.d Ziffer 2.8 ereignet, ist der AG zu einer Kontrolle beim AN vor Ort auch ohne Vorankündigung berechtigt. Der AG ist verpflichtet, alle erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des AN vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages 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 zu 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.
- 7.2 Löschungen nach vorstehendem 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 oder in Textform 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 Regelungen für Schäden, die beim AG durch Verstöße des AN gegen diese AV-Vereinbarung oder die einschlägigen, 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 über 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 Die Einrede des Zurückbehaltungsrechts nach § 273 BGB an den Daten, Teilen davon sowie Datenträgern des AG wird ausgeschlossen.
- 9.2 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.

- 9.3 Eine gesonderte Vergütung für Tätigkeiten des AN, insbesondere Unterstützungsleistungen, nach dieser AV-Vereinbarung fällt nicht an, diese ist vielmehr mit der Vergütung aus dem kommerziellen Vertrag abgegolten.
- 9.4 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 AV-Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 9.5 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 dieser auch für alle Ansprüche oder Angelegenheiten, die sich aus oder im Zusammenhang mit dieser AV-Vereinbarung ergeben.
- 9.6 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
Hier klicken, um Text einzufügen	Hier klicken, um Text einzufügen
Ort, Datum	Ort, Datum
Hier klicken, um Text einzufügen	Hier klicken, um Text einzufügen
Funktion und Name in Druckbuchstaben	Funktion und Name in Druckbuchstaben
Hier Unterschrift einfügen	Hier Unterschrift einfügen
-----	-----
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

ANLAGE 1: Details zur Auftragsverarbeitung (vom AG auszufüllen/vom AN bei Bedarf anzupassen)

Lfd. Nr.	Kurzbeschreibung der Leistungen/Services	Gegenstand und Art der Datenverarbeitung Welche Leistungen die Datenverarbeitung betreffend werden erbracht: Erheben? Speichern? Übermitteln? Wie?	Speichert der AN bei sich die Daten des AG?	Wann erfolgt die Löschung?	Kreis der Betroffenen	Datenkategorien.	Ort (Stadt/Land), in dem der AN die Daten verarbeitet
	BEISPIEL: Druck von Visitenkarten von Mitarbeitern des AG	BEISPIEL: Es sind die zu druckenden personenbezogenen Daten vom AN entgegenzunehmen und aus technischen Zwecken zwischenspeichern. Diese werden dann für den Druck der Visitenkarten verarbeitet und gedruckt.	BEISPIEL: Ja	BEISPIEL: 7 Tage nach Beendigung der Veranstaltung	BEISPIEL: Mitarbeiter des AG	BEISPIEL: Namen, E-Mail-Adressen sowie berufliche Telefonnummern der Mitarbeiter	BEISPIEL: München
In die Tabellenfelder klicken, um Text einzufügen							

ANLAGE 2: Angaben zur Datenschutz-Organisation des AN (vom AN auszufüllen)

a. Weisungsempfänger auf Seiten des AN - Name, Funktion

Hier klicken, um Text einzufügen

b. Datenschutzbeauftragter

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

Hinweis: Für den AG und damit den AN gilt § 38 BDSG (Bundesdatenschutzgesetz). Die Bestellung eines DSB ist danach verpflichtend, wenn der AN mindestens 20 Mitarbeitende hat und bei Kleinbetrieben unter 20 Mitarbeitenden, wenn er Daten nach Art. 9 DSGVO verarbeitet oder Markt-/Meinungsforschung anbietet.

c. Verschwiegenheit u.a.

- ☐ Alle Mitarbeiter des ANs, die mit personenbezogenen Daten des AGs in Berührung kommen können, sind über die für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht, zur Verschwiegenheit und zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet.

d. Datenschutz-Schulungen

- ☐ Die Mitarbeiter des ANs, die mit personenbezogenen Daten des AGs in Berührung kommen können, wurden regelmäßig im Datenschutz geschult.

e. Interne Datenschutz-Kontrollen

- ☐ Der AN führt regelmäßig interne Datenschutz-Kontrollen durch.

f. Zertifizierungen

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

- ☐ Keine
- ☐ Folgende (bitte anhängen und hier benennen):

g. Regelwerk zum Datenschutz

- ☐ Der AN verfügt über dokumentierte interne Regelungen und Weisungen zum Datenschutz und der sicheren Verarbeitung von Informationen.

h. Weiterentwicklung des Datenschutz-Managements

- ☐ Das etablierte Datenschutz-Management des AN wird kontinuierlich weiterentwickelt und verbessert.

i. Pflichtdokumentationen zum Datenschutz

- ☐ Der AN verfügt über eine Dokumentation zum Datenschutz, die die Anforderungen der DSGVO berücksichtigt. Insbesondere verfügt der AN über Datenschutzerklärungen, ein Verzeichnis von Verarbeitungstätigkeiten sowie (sofern zutreffend) über Vereinbarungen zur Auftragsverarbeitung mit etwaigen Dienstleistern.

ANLAGE 3: Ort der Datenverarbeitung durch den AN *(vom AN auszufüllen)*

Erfolgt die Datenverarbeitung durch den AN in oder aus einem Mitgliedstaat der EU, des EWR oder einem Land, für das die Angemessenheit des Datenschutz-Niveaus durch einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 Abs. 3 DS-GVO) festgestellt wurde?

Hinweis: Angaben zum Ort der Datenverarbeitung durch etwaige Unterauftragsverarbeiter machen Sie bitte in Anlage 4.

☐

Ja

☐

Nein

Ist oben „Nein“ anzukreuzen, stimmen die Parteien darin überein, dass zwischen den Vertragsparteien EU-Standardvertragsklauseln abzuschließen sind, es sei denn ein ausreichendes Datenschutz-Niveau

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften beim AN (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO)

☐ wird hergestellt durch: _____

ANLAGE 4: Liste von genehmigten Unterauftragsverarbeitern *(vom AN auszufüllen)*

Werden Unterauftragsverarbeiter eingesetzt? ☐ Nein
☐ Ja

Soweit Unterauftragsverarbeiter eingesetzt werden, sind diese abschließend in folgender Tabelle aufzulisten.

Hinweis: Bitte machen Sie hier nur Angaben zu Datenverarbeitungstätigkeiten, die Sie an Unterauftragsverarbeiter ausgelagert haben. Unterauftragnehmer, die allgemeine Tätigkeiten wie z.B. Organisations- oder Beratungsleistungen ohne Personenbezug erbringen, sind hier nicht zu nennen.

Name des Unterauftragsverarbeiters	Anschrift des Unterauftragsverarbeiters	Aufgabe des Unterauftragsverarbeiters (= welche personenbezogene Daten des AG verarbeitet der Unterauftragsverarbeiter/ hat Zugriff aus welchen Gründen?)
In die Tabellenfelder klicken, um Text einzufügen		

ANLAGE 5: Beschreibung der vom AN zum Schutz der Daten und schützenswerten Informationen des AG getroffenen technischen und organisatorischen Maßnahmen *(vom AN auszufüllen)*

1. Ausfüllhinweis:

Die nachfolgende Tabelle enthält Anforderungen an die vom AN umzusetzenden technischen und organisatorischen Maßnahmen (kurz: TOMs). Durch Markierung der Maßnahmen bestätigt der AN deren Umsetzung.

Fett geschriebene Maßnahmen stellen Mindestanforderungen dar. Sind diese nicht angekreuzt, muss der AN Angaben im Abschnitt „Optional: Kurzbeschreibung zu ...“ vornehmen, um alternative oder ergänzende Maßnahmen zu erläutern, die die eigentliche Mindestanforderung ebenso adäquat erfüllen.

Um die Prüfung dieser Anlage 5 durch den AG zu erleichtern und zu beschleunigen, sollte der Abschnitt „Optional: Kurzbeschreibung zu ...“ auch vom AN genutzt werden, um die vom AN markierten oder darüber hinaus getroffenen Maßnahmen je Gewährleistungsziel kurz zu erläutern.

Bei etwaigem Klärungsbedarf zu diesen Maßnahmen kontaktiert der AN den AG, bevor der Vertrag geschlossen wird.

2. Verantwortungsbereiche bei Fernzugriffs- und anderen Datenübermittlungs-Szenarien

Szenario A: Virtueller Client

a) Beschreibung: Der AN greift über einen vom AG bereitgestellten Fernzugang auf Ressourcen des AG zu. Darin verarbeitet der AN im Rahmen der Leistungserbringung Daten oder schützenswerte Informationen (zusammen in dieser Anlage 5 „**Informationen**“ genannt) des AG.

b) Verantwortungsbereiche: Der AG setzt TOMs nach Stand der Technik für den virtuellen Client und die darin verarbeitbaren Informationen um. Der AN setzt TOMs in seinem Verantwortungsbereich um (insbesondere die Systeme, von denen aus der virtuelle Client des AG genutzt wird).

Szenario B: Cloud-Anwendung

a) Beschreibung: Der AG stellt cloud-basierte Ressourcen bereit, auf die der AN im Rahmen seiner Leistungserbringung zugreift und darin Informationen des AG verarbeitet.

b) Verantwortungsbereiche: Der AG setzt TOMs nach Stand der Technik für die cloud-basierten Ressourcen und die darin verarbeitbaren Informationen um. Der AN setzt TOMs in seinem Verantwortungsbereich um (insbesondere die Systeme, von denen aus die cloud-basierten Ressourcen des AG genutzt und Informationen des AG verarbeitet werden).

Szenario C: E-Mail

a) Beschreibung: AG und AN tauschen Informationen auf elektronischem Wege ausschließlich per E-Mail aus. Für die Leistungserbringung nutzt der AN folglich eigene IT-Anwendungen und -Infrastrukturen.

b) Verantwortungsbereiche: Der AG setzt TOMs nach Stand der Technik für seine E-Mail-Systeme und die darin verarbeitbaren Informationen um. Der AN setzt TOMs in seinem Verantwortungsbereich um (insbesondere die Systeme, auf denen Informationen des AG verarbeitet werden).

Der AN ist folglich bei allen Szenarien in der Pflicht, Aussagen zur Umsetzung der unten aufgeführten technischen und organisatorischen Maßnahmen in seinem Verantwortungsbereich zu machen, damit ein durchgängig hohes Sicherheitsniveau erreicht wird.

Allgemein gilt für die Szenarien A und B:

Der Remote-Zugang (Szenario A) bzw. die cloud-basierte Ressource (Szenario B) wird durch den IT-Betrieb des AG betrieben und überwacht. Für den Zugriff stellt der AG personalisierte Benutzerkennungen bereit. Die Authentisierung erfolgt über Multifaktor-Authentisierung. Dabei werden Anmeldevorgänge, durchgeführte Benutzeraktivitäten sowie sicherheitsrelevante Ereignisse protokolliert und ausgewertet. Die Protokolldaten werden zum Zwecke des sicheren Betriebs verarbeitet. Bei erforderlicher Notwendigkeit kann eine gemeinsame Auswertung der Protokolldaten durch AG und AN erfolgen. Bei Verdacht auf einen Sicherheitsvorfall kann der AG die Verbindung (Szenario A) bzw. den Zugang (Szenario B) unmittelbar trennen und zugehörige Zugänge des AN deaktivieren. Der AN stellt einen Internetzugang bereit, über den der AN auf den Remote-Zugang (Szenario A) bzw. die cloud-basierte Ressource (Szenario B) des AG zugreift. Eine Kostenübernahme für diesen Internetzugang durch den AG findet nicht statt. Der AG stellt dem AN Zugriffsrechte bereit, die auf die zur Aufgabenerfüllung notwendigen Rechte eingeschränkt sind („need to know“-Prinzip).

Kurzbezeichnung	Erläuterung und Beispiele	Beschreibung der konkret vom AN getroffenen Maßnahmen
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)		
Zutrittskontrolle	Dem Stand der Technik entsprechende Maßnahmen, die unbefugte Zutritte zu Datenverarbeitungsanlagen erschweren sowie erkennen können.	<p>Vom AN getroffene Maßnahmen:</p> <p>Umgesetztes Konzept zur physischen Sicherheit <input type="checkbox"/></p> <p>Umgesetztes Zutrittskonzept gemäß „least privilege“ <input type="checkbox"/></p> <p>Perimeterschutz <input type="checkbox"/></p> <p>Einbruchshemmende Fenster und Türen <input type="checkbox"/></p> <p>Begleitung von Besuchern / Fremdpersonal <input type="checkbox"/></p> <p>Protokollierung von Besuchern / Fremdpersonal <input type="checkbox"/></p> <p>Ausweise für Besucher / Fremdpersonal <input type="checkbox"/></p> <p>Dokumentierte Schlüsselverwaltung <input type="checkbox"/></p> <p>Schließanlage mit Sicherheitskreisen <input type="checkbox"/></p> <p>Werkschutz bzw. Pförtner <input type="checkbox"/></p> <p>Alarmanlagen <input type="checkbox"/></p> <p>Videoüberwachung <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Zutrittskontrolle:</p> <p>Hier klicken, um Text einzufügen</p>
Zugangskontrolle	Dem Stand der Technik entsprechende Maßnahmen, die eine unbefugte Systembenutzung erschweren sowie erkennen können.	<p>Vom AN getroffene Maßnahmen:</p> <p>Prozess zur Anlage, Änderung und Löschung von Zugangsmitteln <input type="checkbox"/></p> <p>Vergabe eindeutiger personalisierter Benutzerkennungen <input type="checkbox"/></p> <p>Verwendung starker Passwörter nach Stand der Technik <input type="checkbox"/></p> <p>Zeitnahe Installation sicherheitsrelevanter Updates <input type="checkbox"/></p>

		<p>Mehrfaktorauthentifizierung bei Anmeldung über externe Netze <input type="checkbox"/></p> <p>Mehrfaktorauthentifizierung bei Anmeldung administrativer Kennungen <input type="checkbox"/></p> <p>Technische Durchsetzung der Passwortvorgaben <input type="checkbox"/></p> <p>Verbot der Mehrfachverwendung und Weitergabe von Passwörtern <input type="checkbox"/></p> <p>Sperren inaktiver Sitzungen (automatisch sowie manuell) <input type="checkbox"/></p> <p>Regelungen zur Sperrung kompromittierter Benutzerkonten <input type="checkbox"/></p> <p>Ändern voreingestellter Anmeldedaten <input type="checkbox"/></p> <p>Zugangsbeschränkte & kryptographische Speicherung von Passwörtern <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Zugangs-kontrolle:</p> <p>Hier klicken, um Text einzufügen</p>
Zugriffskontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte	<p>Vom AN getroffene Maßnahmen:</p> <p>Umgesetztes Rollen- und Rechtekonzept nach „least privilege“-Prinzip <input type="checkbox"/></p> <p>Trennung administrativer und nicht-administrativer Tätigkeiten <input type="checkbox"/></p> <p>Datenträgerverschlüsselung bei mobilen Endgeräten <input type="checkbox"/></p> <p>Datenträgerverschlüsselung bei Serversystemen <input type="checkbox"/></p> <p>Programme zum Schutz vor Schadsoftware <input type="checkbox"/></p> <p>Mehrstufige administrative Berechtigungen nach „least privilege“-Prinzip <input type="checkbox"/></p> <p>Kontrolle der vergebenen Rollen und Rechte auf ihre Notwendigkeit <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Zugriffs-kontrolle:</p> <p>Hier klicken, um Text einzufügen</p>
Trennungskontrolle	Getrennte Verarbeitung von Informationen, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;	<p>Vom AN getroffene Maßnahmen:</p> <p>Umgesetztes Mandantenkonzept zur Trennung von Datenbeständen <input type="checkbox"/></p>

		<p>Getrennte Verarbeitung von Test- und Echtdaten <input type="checkbox"/></p> <p>Vergabe von Zugriffsrechten nach dem Prinzip „need to know“ <input type="checkbox"/></p> <p>Sicherstellung der Zweckbindung bei zu trennenden Datenbeständen <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Trennungskontrolle:</p> <p>Hier klicken, um Text einzufügen</p>
Pseudonymisierung und Anonymisierung	<i>Sofern der Zweck der Datenverarbeitung auch mit pseudonymen oder anonymen Daten möglich ist.</i>	<p>Vom AN getroffene Maßnahmen:</p> <p>Ersatz direkter Personenkennungen durch Pseudonyme <input type="checkbox"/></p> <p>Zugriffsschutz für Zuordnungstabellen Pseudonym <=> Echtdaten <input type="checkbox"/></p> <p>Datensparsame Erhebung personenbezogener Attribute <input type="checkbox"/></p> <p>Anonymisierung hochschutzwürdiger personenbezogener Daten <input type="checkbox"/></p> <p>Sensibilisierung des Personals zur Pseudonymisierung <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Pseudonymisierung:</p> <p>Hier klicken, um Text einzufügen</p>
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)		
Weitergabekontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN)	<p>Vom AN getroffene Maßnahmen:</p> <p>Transportverschlüsselte Übertragung von personenbezogenen Daten <input type="checkbox"/></p> <p>Inhaltsverschlüsselte Übertragung von personenbezogenen Daten <input type="checkbox"/></p> <p>Protokollierung von Datenübertragungen (inkl. Auswertung) <input type="checkbox"/></p> <p>Einsatz von Systemen zur Vermeidung von Datenlecks <input type="checkbox"/></p> <p>Sensibilisierung des Personals zur Weitergabekontrolle <input type="checkbox"/></p>

		<p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Weitergabekontrolle:</p> <p>Hier klicken, um Text einzufügen</p>
Eingabekontrolle	<p>Feststellung, ob und von wem Informationen in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement</p>	<p>Vom AN getroffene Maßnahmen:</p> <p>Vergabe von Zugriffsrechten nach dem Prinzip „need to know“ <input type="checkbox"/></p> <p>Protokollierung von Verarbeitungsvorgängen (inkl. Auswertung) <input type="checkbox"/></p> <p>Verifikationen umfangreicher Eingaben <input type="checkbox"/></p> <p>Versionierte Speicherung und Sicherung von Datenbeständen <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Eingabekontrolle:</p> <p>Hier klicken, um Text einzufügen</p>
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)		
Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit	<p>Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), Notfallpläne</p>	<p>Vom AN getroffene Maßnahmen:</p> <p>Regelmäßige Datensicherungen <input type="checkbox"/></p> <p>Redundante IT-Infrastruktur <input type="checkbox"/></p> <p>Notfallmanagement für erwartbare Ausfallszenarien <input type="checkbox"/></p> <p>Bereitstellung von Ausweich-IT-Infrastruktur <input type="checkbox"/></p> <p>Betriebliche Überwachung der IT-Infrastruktur <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zu Verfügbarkeitskontrolle und rascher Wiederherstellbarkeit:</p> <p>Hier klicken, um Text einzufügen</p>

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung und datenschutzfreundliche Voreinstellungen (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)		
Incident-Response-Management		<p>Vom AN getroffene Maßnahmen:</p> <p>Etablierte Prozesse zur Behandlung von Sicherheitsvorfällen <input type="checkbox"/></p> <p>Etablierte Prozesse zur Behandlung von Datenschutzvorfällen <input type="checkbox"/></p> <p>Etabliertes Sicherheitsmonitoring der IT-Infrastruktur <input type="checkbox"/></p> <p>Regelmäßige Übungen der Incident-Response-Prozesse <input type="checkbox"/></p> <p>Durchgängige und nachvollziehbare Dokumentation von Vorfällen <input type="checkbox"/></p> <p>Etablierte Melde- und Eskalationswege <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zum Incident-Response-Management:</p> <p>Hier klicken, um Text einzufügen</p>
Datenschutzfreundliche Voreinstellungen	<i>Sofern der AN Softwareentwicklung oder vergleichbare Dienstleistungen für den AG leistet.</i>	<p>Vom AN getroffene Maßnahmen:</p> <p>Wahrung der Datenminimierung bei der Systemkonfiguration <input type="checkbox"/></p> <p>Wahrung der Zweckbindung bei der Systemkonfiguration <input type="checkbox"/></p> <p>Wahrung der Speicherfristen bei der Systemkonfiguration <input type="checkbox"/></p> <p>Opt-in zu erweiterten Verarbeitung personenbezogener Daten <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zu datenschutzfreundlichen Voreinstellungen:</p> <p>Hier klicken, um Text einzufügen</p>
Auftragskontrolle	<i>Sofern der AN selbst Auftragsverarbeiter als Unterauftragnehmer einsetzt: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.</i>	<p>Vom AN getroffene Maßnahmen:</p> <p>Definierte Auswahlkriterien für Unterauftragnehmer <input type="checkbox"/></p> <p>Datenschutz-Management von Auftragsverhältnissen <input type="checkbox"/></p> <p>Transparenz bei Nennung eingesetzter Unterauftragnehmer <input type="checkbox"/></p> <p>Prozesse zur Kontrolle von Unterauftragnehmern <input type="checkbox"/></p>

		<p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Auftragskontrolle:</p> <p>Hier klicken, um Text einzufügen</p>
Evaluierung	<p>Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung.</p>	<p>Vom AN getroffene Maßnahmen:</p> <p>Regelmäßige interne Auditierung und Überprüfung von Maßnahmen <input type="checkbox"/></p> <p>Durchführung von Penetrationstests <input type="checkbox"/></p> <p>Prozess zur kontinuierlichen Verbesserung der Informationssicherheit <input type="checkbox"/></p> <p>Prozesse zur Evaluierung von Unterauftragnehmern <input type="checkbox"/></p> <p>Optional: Kurzbeschreibung alternativer oder ergänzender Maßnahmen des AN zur Evaluierung:</p> <p>Hier klicken, um Text einzufügen</p>