Vereinbarung über eine Auftragsverarbeitung

Web Computing GmbH (März 2024)

1. Zweck und Anwendungsbereich

1.1. **Zweck.** Mit dieser Vereinbarung über eine Auftragsverarbeitung („**AVV**“) möchten die Parteien die Einhaltung von Artikel 28 Absätze 3 und 4 der 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 („**DS-GVO**“) bei der Verarbeitung personenbezogener Daten im Rahmen des zwischen den Parteien abgeschlossenen Hauptvertrages („**Vertrag**“) sicherstellen.

1.2. **Einhaltung des Datenschutzes.** Die AVV entbindet die Parteien nicht von ihren sonstigen gesetzlichen Pflichten, einschließlich der rechtmäßigen Verarbeitung personenbezogener Daten. Sie stellen für sich allein die Erfüllung der Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen nicht sicher.

1.3. **Definitionen.** Soweit Begrifflichkeiten in dieser AVV nicht abweichend definiert sind, gelten für sie die Definitionen des Vertrages. „**Auftragsverarbeiter**“ im Sinne dieser AVV meint die Web Computing. „**Verantwortlicher**“ im Sinne dieser AVV meint den Kunden.

1.4. **Anlagen zur AVV.** Die folgenden Anlagen sind Bestandteil dieser AVV:

- Anlage 1 (Beschreibung der Verarbeitungstätigkeiten)
- Anlage 2 (Technische und organisatorische Maßnahmen)
- Anlage 3 (Liste der Unterauftragsverarbeiter)

2. Unabänderbarkeit der AVV

2.1. **Keine Änderung.** Die Parteien verpflichten sich, Regelungen der AVV nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anlagen angegebenen Informationen.

2.2. **Ergänzungen**. Vorstehende Regelung in Ziffer 2.1 hindert die Parteien nicht daran, die in dieser AVV festgelegten Bestimmungen in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Regelungen der AVV stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

3. Auslegung

3.1. **Begriffe.** Werden in dieser AVV die in der DS-GVO bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

3.2. **Auslegung.** Diese Klauseln sind im Lichte der Bestimmungen der DS-GVO bzw. der Verordnung (EU) 2018/1725 auszulegen.

3.3. **Schutz der Grundrechte.** Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der DS-GVO oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

4. Vorrang

Im Fall eines Widerspruchs zwischen Regelungen dieser AVV und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben die Regelungen dieser AVV Vorrang.

5. Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anlage 1 (Beschreibung der Verarbeitungstätigkeiten) aufgeführt.

6. Weisungen

6.1. **Dokumentation.** Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren, insbesondere wenn die Weisung mündlich erteilt wurde. Im Fall einer mündlichen Weisung hat der Auftragsverarbeiter den Eingang der Weisung dem Verantwortlichen in Textform zu bestätigen.

6.2. **Rechtswidrigkeit einer Weisung.** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DS-GVO, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

6.3. **Kosten.** Weisungen des Verantwortlichen dürfen ausschließlich die Verarbeitung von personenbezogenen Daten und keine anderen Aspekte des Vertrages betreffen. Soweit

Weisungen zu zusätzlichem Aufwand bei dem Auftragsverarbeiter führen, ist der Auftragsverarbeiter berechtigt, neben dem Ersatz von nachgewiesenen Auslagen eine angemessene Vergütung für die Ausführung der Weisung zu verlangen.

7. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für die in Anlage 1 (Beschreibung der Verarbeitungstätigkeiten) genannten spezifischen Zwecke, sofern er keine weiteren Weisungen des Verantwortlichen erhält.

8. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anlage 1 (Beschreibung der Verarbeitungstätigkeiten) angegebene Dauer verarbeitet.

9. Sicherheit der Verarbeitung

9.1. **Technische und organisatorische Maßnahmen.** Der Auftragsverarbeiter ergreift mindestens die in Anlage 2 (Technische und organisatorische Maßnahmen) aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt („**Verletzung des Schutzes personenbezogener Daten**“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken für die Rechte und Freiheiten und den unterschiedlichen Eintrittswahrscheinlichkeiten gebührend Rechnung. Die Maßnahmen sind so zu wählen, dass eine sofortige Feststellung von Verletzungen des Schutzes personenbezogener Daten möglich ist.

9.2. **Technischer Fortschritt.** Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer kontrolliert die getroffenen Maßnahmen regelmäßig dahingehend, ob sie ein noch angemessenes Schutzniveau erreichen. Um ein angemessenes Schutzniveau sicherzustellen, ist es dem Auftragsverarbeiter gestattet, die in Anlage 2 (Technische und organisatorische Maßnahmen) aufgeführten technischen und organisatorischen Maßnahmen zugunsten eines gesteigerten Schutzniveaus zu anzupassen, wenn die Änderung dokumentiert und dem Verantwortlichen vor Eintritt der Änderung zur Verfügung gestellt wird.

9.3. **Verpflichtung zur Vertraulichkeit.** Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

10. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische 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 („**sensible Daten**“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

11. Dokumentation und Einhaltung der Klauseln

11.1. **Nachweis.** Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

11.2. **Bearbeitung von Anfragen.** Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

11.3. **Bereitstellung von Informationen.** Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anforderung alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DS-GVO und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Dies betrifft insbesondere die Einhaltung der technischen und organisatorischen Maßnahmen in Anlage 2 (Technische und organisatorische Maßnahmen). Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten stichprobenartig in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen durch IT-Sicherheits- oder Datenschutzaudits (beispielsweise nach BSI-Grundschutz), aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (beispielsweise Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutz-auditoren, Qualitätsauditoren) des Auftragsverarbeiters

berücksichtigen. Sofern vorhanden, können auch Zertifizierungen nach Art. 42 DS-GVO zum Nachweis dienen, ebenso wie Nachweise zum Einhalt genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.

11.4. **Durchführung der Überprüfung.** Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung, das heißt zumindest einundzwanzig (21) Kalendertage im Voraus, durchgeführt.

11.5. **Kosten der Überprüfung.** Die Kosten und Aufwände für die Prüfung trägt der Verantwortliche, wobei sich die Kosten und Aufwände anhand den jeweils zwischen den Parteien vereinbarten Konditionen und den nachgewiesenen Aufwänden bemessen. Sind keine Konditionen vereinbart, ist der Auftragsverarbeiter berechtigt, eine angemessene Vergütung zu verlangen.

11.6. **Information der Aufsichtsbehörde.** Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

12. Einsatz von Unterauftragsverarbeitern

12.1. **Unterauftragsverhältnis.** Als Unterauftragsverhältnis sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Verarbeitungstätigkeit beziehen und von einem Dritten („**Unterauftragsverarbeiter**“) durchgeführt werden. Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens einen Monat im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen angemessene Zeit (in der Regel zwei Wochen) ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Der Verantwortliche darf ein Widerspruchsrecht nur dann ausüben, wenn objektive Zweifel an der datenschutzrechtlichen Zuverlässigkeit des Unterauftragsverarbeiters bestehen. Im Fall eines zulässigen Widerspruchs, ist der Verantwortliche entsprechend der Regelungen des Vertrages, insbesondere der AVB, zur Kündigung wegen Leistungsänderung berechtigt.

12.2. **Verpflichtung zum Datenschutz.** Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß dieser AVV gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend dieser AVV und gemäß der DS-GVO und/oder der Verordnung (EU) 2018/1725 unterliegt.

12.3. **Kopie der Unterbeauftragung.** Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

12.4. **Verantwortlichkeit.** Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen entsprechend den Haftungsvereinbarungen des Vertrages , insbesondere des Bestellscheins und der AVB, dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

12.5. **Drittbegünstigung.** Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

13. Internationale Datenübermittlung

13.1. **Grundsatz.** Die Datenverarbeitung findet grundsätzlich ausschließlich in einem Mitgliedsstaat der europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

13.2. **Übermittlung in Drittland.** Eine Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage

dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DS-GVO oder der Verordnung (EU) 2018/1725 im Einklang stehen.

13.3. **EU Standardvertragsklauseln.** Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DS-GVO beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DS-GVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der DS-GVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

14. Unterstützung des Verantwortlichen

14.1. **Betroffenenanträge.** Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt. Insbesondere sind die eigenmächtige Löschung und Einschränkung der Verarbeitung durch den Auftragsverarbeiter nicht gestattet.

14.2. **Unterstützung bei Betroffenenanträgen.** Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter stellt dem Verantwortlichen unverzüglich sämtliche relevante Informationen zur Verfügung, insbesondere solche Informationen, die es zur Erfüllung von Informationspflichten bedarf.

14.3. **Sonstige Unterstützung.** Ungeachtet der Pflicht des Auftragsverarbeiters, den Verantwortlichen bei Betroffenenanträgen zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

- Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten („**Datenschutz-Folgenabschätzung**“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
- Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
- Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
- Verpflichtungen gemäß Artikel 32 DS-GVO.

14.4. **Vereinbarung über Unterstützung.** Die Parteien legen in Anlage 2 (Technische und organisatorische Maßnahmen) die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

14.5. **Aufsichtsbehördliche Maßnahmen**. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörden, sofern sie die Ausführung dieser Klauseln betreffen. Dies gilt auch für Ordnungswidrigkeits- und Strafverfahren.

14.6. **Kosten.** Der Auftragsverarbeiter ist berechtigt, für Unterstützungshandlungen eine angemessene Vergütung entsprechend der vertraglich vereinbarten Vergütungsregelungen zu verlangen.

15. Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Fall einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der DS-GVO oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

16. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Fall einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

16.1. bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

16.2. bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 DS-GVO in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

- die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

16.3. Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

16.4. bei der Einhaltung der Pflicht gemäß Artikel 34 DS-GVO, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

17. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

17.1. **Inhalt der Meldung.** Im Fall einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

18. Verstöße gegen diese AVV

Falls der Auftragsverarbeiter seinen Pflichten gemäß dieser AVV nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der DS-GVO und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er die Bestimmungen dieser AVV einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

19. Beendigung des Vertrages

19.1. **Beendigung bei Vertragsende.** Wird der dieser AVV zugrunde liegende Vertrag beendet, so endet auch diese AVV.

19.2. **Kündigungsrecht des Verantwortlichen.** Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß dieser AVV betrifft, wenn

- der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter wegen eines wesentlichen Verstoßes gegen diese AVV ausgesetzt hat und die Einhaltung der Regelungen dieser AVV nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
- der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese AVV verstößt oder seine Verpflichtungen gemäß der DS-GVO und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
- der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die

seine Pflichten gemäß diesen Klauseln, der DS-GVO und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

19.3. **Kündigungsrecht des Auftragsverarbeiters.** Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß dieser AVV betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen und/oder den Vertrag verstoßen.

19.4. **Außerordentliche Kündigung.** Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

19.5. **Pflicht bei Beendigung.** Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen in Textform, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, insbesondere Sicherheitskopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten über das Beendigung des Vertrages hinaus besteht. Dies gilt auch für Test- und Ausschussmaterial. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung der Regelungen dieser AVV. Entscheidet sich der Verantwortliche für eine Löschung der Daten, so teilt der Auftragsverarbeiter dem Verantwortlichen auf Anfrage Zeitpunkt und Umstände der Löschung mit.

19.6. **Aufbewahrung von Dokumentationen.** Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen und nicht Teil der Datenverarbeitung sind, sind durch den Auftragsverarbeiter entsprechend den Aufbewahrungspflichten aufzubewahren. Der Auftragsverarbeiter kann die zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

20. Schlussbestimmungen

20.1. **Kontakt.** Als Kontaktperson für diese AVV und den Datenschutz werden die im Bestellschein benannten Personen benannt.

20.2. **Deutsches Recht.** Für alle Streitigkeiten aus oder im Zusammenhang mit dieser AVV, einschließlich dieser AVV selbst gilt das Recht der Bundesrepublik Deutschland.

20.3. **Geltung der vertraglichen Regelungen.** Die Regelungen des Vertrages, insbesondere solche der Allgemeinen Vertragsbedingungen der Web Computing, finden im Übrigen Anwendung.

Anlage 1 (Beschreibung der Verarbeitungstätigkeiten)

abgestimmt zwischen den Vertragspartnern am xx. xxxxx xxxx yy:yy Uhr

Die folgenden Angaben sind bei Bedarf durch den Kunden auszufüllen. Zur Unterstützung hat Web Computing bereits Daten und Informationen aufgeführt, die basierend auf dem Standardverhalten der Software voraussichtlich zu verarbeiten sind. Hierbei handelt es sich jedoch nicht um eine vollständige Auflistung, da die Verarbeitungstätigkeiten vom Use Case des Kunden abhängen.

1. **Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:**

   - Beschäftigte des Verantwortlichen bzw. Kunden
   - *Bei Bedarf vom Kunden zu erweitern, ansonsten bitte diesen Stichpunkt löschen*

2. **Kategorien personenbezogener Daten, die verarbeitet werden:**

   Für coovi:
   - Name, Kennung/ID, E-Mail-Adresse und Authentifizierungsinformationen der coovi-Benutzer
   - IP-Adressen
   - Inhalte von Logs
   - *Bei Bedarf vom Kunden zu erweitern, ansonsten bitte diesen Stichpunkt löschen*
     Hinweis: In coovi können Bilder und Videos hochgeladen bzw. erstellt werden. Die so resultierenden Video-, Audio- und Bilddaten können personenbezogene Daten beinhalten, z. B. wenn ein Video selbst besprochen und der Sprecher dabei aufgenommen wird.

   Für DialogBits:
   - Name, Kennung/ID, E-Mail-Adresse und Authentifizierungsinformationen der Nutzer des “DialogBits Managers”
   - IP-Adressen
   - Inhalte von Logs
   - *Bei Bedarf vom Kunden zu erweitern, ansonsten bitte diesen Stichpunkt löschen*
     Hinweis: Alle Benutzereingaben bzw. -Interaktionen (inkl. erstellte Analyse-Events), die über den Chatbot getätigt werden, sowie Antworten des Chatbots werden verarbeitet. Je nach Kunden-Use-Case könnten diese Informationen personenbezogene Daten enthalten.

3. **Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. 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 oder zusätzliche Sicherheitsmaßnahmen:**

   Keine
   Bei Bedarf vom Kunden anzupassen, ansonsten bitte diesen Hinweis löschen.

4. **Art der Verarbeitung:**
   Die Arten der Verarbeitung umfassen alle Arten im Sinne der DSGVO, insbesondere:
   - das Erheben und Erfassen personenbezogener Daten zur Zweckerfüllung.
   - das Speichern, Auslesen und Abfragen gespeicherter personenbezogener Daten.
   - das Offenlegen durch Übermittlung von personenbezogene Daten an relevante Unterauftragnehmer.
   - das Löschen und Vernichten nicht länger für die Zweckerfüllung benötigter personenbezogener Daten.

5. **Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:**
   Personenbezogene Daten werden zum Zweck der Bereitstellung der coovi- bzw. DialogBits-Plattform mitsamt aller vereinbarten Funktionalitäten in Übereinstimmung mit dem Vertrag verarbeitet.

6. **Dauer der Verarbeitung:**
   Bis zur Beendigung des zugehörigen Lizenzvertrages.

Anlage 2 (Technische und organisatorische Maßnahmen)

1. Vertraulichkeit

a) Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Das Bürogebäude ist mittels eines Schließsystems mit elektronischem Türöffner gesichert.
- Die zum Schließsystem gehörenden Schlüssel werden einzeln ausgegeben. Die Ausgabe wird dokumentiert, inkl. Zuordnung der Schlüssel zu den Personen.
- Das Bürogebäude ist über eine Einbruchmeldeanlage gegen unbefugten Zutritt gesichert.
- Zutritt für Besucher erfolgt nur anhand einer definierten Richtlinie, die z. B. die Pflicht zum Eintrag in das Besucherbuch und das Tragen eines Besucherausweises vorschreibt.

b) Zugangskontrolle

- Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben: Persönlicher und individueller User-Log-In bei Anmeldung auf dem zugeordneten Dienst-Systemen bzw. bei Anmeldungen auf Anwendungen auf Servern im Unternehmensnetzwerk
- Nur autorisierte Nutzer haben Zugangsberechtigungen zu Serversystemen.
- Der Zugang zu Servern und Anwendung erfordert den Einsatz sicherer Passwörter.
- Unternehmenspasswörter werden über einen Passwort-Manager verwaltet, der die Passwörter verschlüsselt abspeichert.
- Der Zugriff auf Server und Anwendungen erfordert wenn möglich eine Multi-Faktor-Authentifizierung.
- Auf unseren Servern wird eine Firewall zum Filtern von validen IP-Adressen und Ports eingesetzt.
- Der Zugriff auf Server ist nur über einen definierten Zugriffspunkt (Jumpserver) möglich.
- Der administrative Zugang ist nur von freigegebenen IP-Adresse möglich.

c) Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Verwaltung und Dokumentation von differenzierten Berechtigungen
- Mobile Datenträger können bei Bedarf verschlüsselt werden.
- Dienstgeräte wie Notebooks und Smartphones werden mittels einer Mobile-Device-Management-Lösung verwaltet.
- Akten und Datenträger werden gemäß DIN 66399 fachkundig entsorgt.

d) Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Die Entwicklungs- und Produktionsumgebungen sind voneinander getrennt.
- Die Anwendungen implementieren eine Mehrmandantenfähigkeit über eine logische Mandantentrennung zwischen den unterschiedlichen Kunden.

2. Integrität

a) Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- E-Mails bzw. E-Mail-Anhänge werden bei Bedarf Ende-zu-Ende verschlüsselt übertragen. Eine Transportverschlüsselung (HTTPS) besteht grundsätzlich.
- Verschlüsselung des Speichermediums von Dienst-Notebooks
- Für den Datei- und Datentransfer zwischen Systemen über eine Netzwerkverbindung wird eine Verschlüsselung wie TLS oder SFTP verwendet.
- In den Büroräumen wird ein gesichertes WLAN eingesetzt.
- Für Besucher ist ein separates Gäste-WLAN eingerichtet.

b) Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Vergabe von Zugriffsrechten nach Zuständigkeit.
- Zuständigkeiten werden organisatorisch festgelegt

3. Verfügbarkeit und Belastbarkeit

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Implementierung und stetige Weiterentwicklung eines Sicherheitskonzeptes für Software- und IT-Anwendungen.

- Einrichtung von Backup-Verfahren zur Vermeidung größerer Datenverluste im Notfall.
- Regelmäßige Aktualisierung der Software-Komponenten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a) Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis bei deren Einstellung
- Hinreichende und regelmäßig wiederholende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- Durchführung von regelmäßigen Audits des Datenschutzbeauftragten nach Art. 32 DS-GVO zur Sicherheit der Verarbeitung

b) Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Durch datenschutzfreundliche Voreinstellungen wird sichergestellt, dass möglichst nur benötigte Daten verarbeitet werden, um die Datenminimierung zu gewährleisten.

- DialogBits: Insbesondere Aufzeichnung bzw. Analyse von Chatbot-Gesprächsprotokollen kann selbstständig konfiguriert oder gänzlich deaktiviert werden.
- coovi: Verschiedene konfigurierbare Voreinstellungen sind möglich, z.B. Gästezugriff, Ausschluss von Dimensionen in der Analysefunktion und weitere Einstellungen.
- Kein Tracking durch Drittanbieter bei Aufruf z. B. eines DialogBits-Chatbots bzw. coovi-Videos
- Unterscheidung zwischen optionalen und Pflichteingabefeldern bei Web-Formularen

d) Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- Verpflichtung der Mitarbeiter auf das Datengeheimnis

Bei der Auswahl unserer Unterauftragnehmer favorisieren wir jene mit angemessenen Zertifizierungen (z. B. **ISO 27001**). Insbesondere jene Unterauftragnehmer, die für das Hosting unserer Plattformen zuständig sind und damit im Besonderen zugehörige Daten verarbeiten, weisen eine entsprechende Zertifizierung auf (vgl. Anlage 3).

Anlage 3 (Liste der Unterauftragsverarbeiter)

A. Für Leistungen „DialogBits“:

Anbieter	Adresse	Zweck	Anmerkungen	Zertifizierungen
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Hosting der DialogBits-Plattform, sodass der Cloud-Betrieb möglich ist.		ISO/IEC 27001:2013
Schwarz IT KG	Stiftsbergstraße 1 74172 Neckarsulm Deutschland	Hosting der DialogBits-Plattform, sodass der Cloud-Betrieb möglich ist.	Verwendung des Cloud-Providers “StackIT”	ISO/IEC 27001:2017 ISO/IEC 20000-1:2018
AudioCodes	AudioCodes, Germany GmbH Hanauer Landstraße 148a 60314 Frankfurt am Main Deutschland AudioCodes Ltd. 1 Hayarden Street Airport City Lod 7019900 Israel	Mögliches Telefon-Gateway zur Einbindung des Telefoniekanals als Möglichkeit, mit dem Chatbot zu kommunizieren.	Wird nur benötigt, wenn der Telefoniekanal aktiviert wird. Zudem kann Twillio als Alternative verwendet werden. Vgl. 15.3 Leistungsbeschreibung.	ISO 9001:2015
Twilio Ireland Limited	3 Dublin Landings North Wall Quay Dublin 1 Ireland	Mögliches Telefon-Gateway zur Einbindung des Telefoniekanals als Möglichkeit, mit dem Chatbot zu kommunizieren.	Wird nur benötigt, wenn der Telefoniekanal aktiviert wird. Zudem kann Audiocodes als Alternative verwendet werden. Vgl. 15.3 Leistungsbeschreibung.	ISO/IEC 27001 ISO/IEC 27017 ISO/IEC 27018
WhatsApp Ireland Limited	4 Grand Canal Square, Grand Canal, Harbour, Dublin 2, Irland	Einbindung von WhatsApp als Kanal, um mit dem Chatbot über WhatsApp zu kommunizieren.	Wird nur verwendet, wenn der WhatsApp-Kanal freigeschaltet ist. Nur in Kombination mit Twillio möglich. Vgl. 15.4 Leistungsbeschreibung.	-
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5 80807 München Deutschland	Möglicher Anbieter von generativer KI (LLMs) im Cloud-Setup.	Wird nur verwendet, wenn die generative KI im Dialogmodell konfiguriert ist und dieser Anbieter ausgewählt wurde. Zudem kann OpenAI als Alternative verwendet werden. Mögliche Azure-Regionen umfassen “West	ISO/IEC 27001:2022 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 27701:2019 ISO 9001:2015 ISO 22301:2019 ISO/IEC 20000-1:2018

			Europa" und "Frankreich Mitte". Vgl. 16.2 Leistungsbeschreibung.	

B. Für Leistungen „coovi":

Anbieter	Adresse	Zweck	Anmerkungen	Zertifizierungen
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Hosting der coovi-Plattform, sodass der Cloud-Betrieb möglich ist.		ISO/IEC 27001:2013
Schwarz IT KG	Stiftsbergstraße 1 74172 Neckarsulm Deutschland	Hosting der coovi-Plattform, sodass der Cloud-Betrieb möglich ist.	Verwendung des Cloud-Providers "StackIT", zukünftig geplante Verwendung	ISO/IEC 27001:2017 ISO/IEC 20000-1:2018
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg Luxemburg	Möglicher Anbieter für folgende Funktionen: Text-to-Speech, Speech-to-Text für Untertitel und Suche, Automatische Übersetzungen	Wird nur verwendet, wenn Vertragsbestandteil. Vgl. Video-Erstellung/-Bearbeitung, Punkt 12 Leistungs-beschreibung	ISO/IEC 27001:2022 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 27701:2019 ISO 9001:2015 ISO 22301:2019 ISO/IEC 20000-1:2018
Google Cloud EMEA Limited	Valesco Clanwilliam Place Dublin 2 Ireland	Möglicher Anbieter für folgende Funktionen: Text-to-Speech, Speech-to-Text für Untertitel und Suche, Automatische Übersetzungen	Wird nur verwendet, wenn Vertragsbestandteil. Vgl. Video-Erstellung/-Bearbeitung, Punkt 12 Leistungs-beschreibung	ISO/IEC 27001:2022 ISO/IEC 27017:2015 ISO 9001:2015 ISO 22301:2019
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5 80807 München Deutschland	Möglicher Anbieter für folgende Funktionen: Text-to-Speech, Speech-to-Text für Untertitel und Suche, Automatische Übersetzungen	Wird nur verwendet, wenn Vertragsbestandteil. Vgl. Video-Erstellung/-Bearbeitung, Punkt 12 Leistungs-beschreibung	ISO/IEC 27001:2022 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 27701:2019 ISO 9001:2015 ISO 22301:2019 ISO/IEC 20000-1:2018