VEREINBARUNG ÜBER DIE AUFTRAGSVERARBEITUNG

whatchado GmbH, FN 373602s, Möllwaldplatz 4/39, 1040 Wien, (nachfolgend „Auftragsverarbeiter“ genannt) schließt mit dem Geschäftspartner einen Vertrag (nachfolgend „Hauptvertrag“ genannt) über die Einrichtung eines Unternehmensprofils auf der Website www.whatchado.com (nachfolgend „Website“ genannt). Der Hauptvertrag liegt diesem Vertrag über die Auftragsverarbeitung (nachfolgend „AVV“ genannt) zu Grunde. Art, Zweck und Gegenstand des Hauptvertrages ist die Erbringung von Dienstleistungen im Rahmen der Website als Plattform für Darstellung und Information über Unternehmen, deren Betätigungsfeld, Jobmöglichkeiten und Mitarbeiter. Dies umfasst auch die Veröffentlichung von Videos und Medieninhalten des Geschäftspartners (zusammen nachfolgend die „Services“ genannt). Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten des Geschäftspartners und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers.

Der Auftragsverarbeiter wird die personenbezogenen Daten des Geschäftspartners für die Erbringung der Services gemäß der Beschreibung im Hauptvertrag, den spezifischen Allgemeinen Geschäftsbedingungen zum Hauptvertrag und der Nutzung der Videos („Fremdcontent“) durch den Auftragsverarbeiter und den Ergänzungen und Angaben in diesem AVV verarbeiten. Die Parteien vereinbaren den vorliegenden AVV um sicherzustellen, dass die Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter im Auftrag des Geschäftspartners nach Maßgabe der geltenden Datenschutzgesetze erfolgt.

Sämtliche in diesem AVV verwendeten Begriffe sind im Sinne der EU Datenschutz-Grundverordnung (EU/2016/679, nachfolgend „DSGVO“) zu verstehen, sofern nicht ausdrücklich abweichend vereinbart.

1. Verarbeitung personenbezogener Daten

1.1 Der Auftragsverarbeiter ist Auftragsverarbeiter iSd Artikel 4 Z 8, 28 DSGVO für die Verarbeitung der personenbezogenen Daten des Geschäftspartners. Der Geschäftspartner ist entweder der alleinige Verantwortliche im Hinblick auf die personenbezogenen Daten des Geschäftspartners oder wurde von den relevanten sonstigen Verantwortlichen angewiesen und hat von diesen die Genehmigung eingeholt, der Verarbeitung der personenbezogenen Daten des Geschäftspartners durch den Auftragsverarbeiter gemäß den Angaben in diesem AVV zuzustimmen. Sofern es noch weitere Verantwortliche gibt, wird der Geschäftspartner diese vor Übermittlung von deren personenbezogenen Daten identifizieren und dem Auftragsverarbeiter mitteilen.

1.2 Der Auftragsverarbeiter verpflichtet sich zur Einhaltung aller für ihn in Bezug auf die Services geltenden Datenschutzgesetze und -verordnungen (nachfolgend auch kollektiv „Datenschutzgesetze“). Der Auftragsverarbeiter ist jedoch weder für die Ermittlung der für den Geschäftspartner anwendbaren gesetzlichen Anforderungen verantwortlich noch dafür, dass die durch den Auftragsverarbeiter erbrachten Services diesen Anforderungen entsprechen. Im Hinblick auf das Verhältnis zwischen den Parteien ist der Geschäftspartner für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten des Geschäftspartners verantwortlich.

1.3 Der Geschäftspartner ist einziger Ansprechpartner für den Auftragsverarbeiter. Da sonstige Verantwortliche gegebenenfalls über bestimmte direkte Rechte gegenüber dem Auftragsverarbeiter verfügen, verpflichtet sich der Geschäftspartner, diese Rechte in deren Namen auszuüben und alle hierzu erforderlichen Genehmigungen von den sonstigen Verantwortlichen einzuholen. Gleichermaßen ist der Auftragsverarbeiter einziger Ansprechpartner für den Geschäftspartner in Bezug auf seine Pflichten als Auftragsverarbeiter im Rahmen dieser AVV.

1.4 Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Geschäftspartners gemäß den schriftlichen Weisungen des Geschäftspartners. Eine Verarbeitung für eigene Zwecke des Auftragsverarbeiters findet nicht statt und ist von diesem auch nicht gewünscht. Der Umfang der Weisungen des Geschäftspartners für die Verarbeitung personenbezogener Daten des Geschäftspartners wird durch den Hauptvertrag, diesen AVV einschließlich des Appendix festgelegt. Der Geschäftspartner kann weitere Weisungen erteilen, soweit dies erforderlich ist (ergänzende Weisungen). Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO verstößt, wird der Auftragsverarbeiter den Geschäftspartner unverzüglich darüber informieren. Der Auftragsverarbeiter kann die Erfüllung einer solchen ergänzenden Weisung aussetzen, bis der Geschäftspartner entweder deren Rechtmäßigkeit schriftlich bestätigt oder diese ändert. Sollte der Auftragsverarbeiter den Geschäftspartner informieren, dass einer ergänzenden Weisung nicht entsprochen werden kann, verpflichten sich die Parteien, sich einvernehmlich zu einigen.

1.5 Listen der Kategorien betroffener Personen, der Arten personenbezogener Daten des Geschäftspartners, der besonderen Kategorien personenbezogener Daten und der Verarbeitungstätigkeiten sind im Appendix enthalten. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2. Technische und organisatorische Maßnahmen

2.1 Der Auftragsverarbeiter wird in seinem Verantwortungsbereich gemäß den Angaben im Appendix technische und organisatorische Maßnahmen implementieren und aufrechterhalten, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Nachdem die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen, behält sich der Auftragsverarbeiter das Recht vor, diese Maßnahmen zu ändern, sofern die Funktionalität und Sicherheit der Services nicht negativ beeinträchtigt werden.

2.2 Der Geschäftspartner bestätigt, dass die technischen und organisatorischen Maßnahmen unter Berücksichtigung der Risiken der Verarbeitung der personenbezogenen Daten des Geschäftspartners ein angemessenes Schutzniveau für die personenbezogenen Daten des Geschäftspartners bieten.

3. Unterstützung

3.1 Der Auftragsverarbeiter unterstützt den Geschäftspartner nach Möglichkeit mit technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Verpflichtungen zur Einhaltung der Betroffenenrechte und bei der Einhaltung seiner Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Mitteilung und Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten und die Durchführung einer Datenschutz-Folgenabschätzung unter Berücksichtigung der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

3.2 Der Geschäftspartner wird im Rahmen dieser AVV benötigte Unterstützung durch den Auftragsverarbeiter schriftlich anfordern. Abweichend von den Regelungen des Hauptvertrages hat der Auftragsverarbeiter für seine im Rahmen dieser AVV erbrachten Leistungen, insb. bei der Erfüllung von Unterstützungsleistungen und ergänzenden Weisungen, Anspruch auf folgende Vergütung: Die vom Auftragsverarbeiter erbrachten Leistungen werden grundsätzlich nach Zeithonorar auf Basis von Stundensätzen verrechnet. Verrechnet wird die Gesamtzeit, die der Auftragsverarbeiter (und jeder seiner im Rahmen dieses AVV eingesetzten Mitarbeiter und/oder Sub-Auftragsnehmer) der vertragsgegenständlichen Tätigkeit widmet, wobei insbesondere auch Überarbeitungen von Software-Applikationen und schriftlichen Dokumenten abgerechnet werden. Als Stundensatz werden EUR 95,- pro Beratungsstunde zuzüglich Umsatzsteuer vereinbart. Verrechnet wird nach tatsächlich geleisteter Echtzeit, wobei die abrechenbare Leistungszeit vom Auftragsverarbeiter in 10-Minuten-Schritten erfasst wird. Der Auftragsverarbeiter wird detaillierte Leistungszeitnachweise führen. Rechnungen sind an den Sitz des Geschäftspartners mitsamt des jeweiligen Leistungsnachweises zu senden.

4. Anforderungen Dritter und Vertraulichkeit

4.1 Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten des Geschäftspartners nicht gegenüber Dritten offenzulegen, es sei denn, der Geschäftspartner hat dies gestattet oder es ist gesetzlich erforderlich. Sollte eine Behörde oder Aufsichtsbehörde Zugriff auf personenbezogene Daten des Geschäftspartners anfordern, wird der Auftragsverarbeiter den Geschäftspartner vor der Offenlegung entsprechend informieren, sofern dies nicht gesetzlich verboten ist.

4.2 Der Auftragsverarbeiter verpflichtet alle Mitarbeiter, die Zugang zu personenbezogenen Daten des Geschäftspartners haben, diese Daten vertraulich zu behandeln und unterwirft diese inhaltlich dem Datengeheimnis gemäß § 6 DSG bzw. Art 28 Abs 3 lit b DSGVO. Gleiches gilt im Hinblick auf die Verpflichtung, personenbezogene Daten des Geschäftspartners ausschließlich auf dessen Weisung zu verarbeiten, es sei denn, dass der Auftragsverarbeiter nach geltendem Recht zur Verarbeitung verpflichtet ist.

5. Audit

5.1 Der Auftragsverarbeiter wird Überprüfungen und/oder Inspektionen, die vom Geschäftspartner oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, wie folgt ermöglichen und dazu beitragen:

a) Auf schriftliche Anfrage des Geschäftspartners stellt der Auftragsverarbeiter dem Geschäftspartner oder dem vom Geschäftspartner beauftragten Prüfer die jeweils aktuellen Zertifizierungen und/oder zusammenfassenden Prüfberichte bereit, die vom Auftragsverarbeiter beauftragt wurden, um die Effektivität der technischen und organisatorischen Maßnahmen regelmäßig zu testen, zu beurteilen und auszuwerten.

b) Der Auftragsverarbeiter wird in angemessenem Umfang mit dem Geschäftspartner zusammenarbeiten, indem er zusätzliche verfügbare Informationen in Bezug auf die technischen und organisatorischen Maßnahmen bereitstellt, um den Geschäftspartner zu unterstützen, diese Maßnahmen besser nachzuvollziehen.

c) Sollte der Geschäftspartner weitere Informationen benötigen, um seine eigenen Auditverpflichtungen zu erfüllen oder der Anforderung einer zuständigen Aufsichtsbehörde gerecht zu werden, wird er den Auftragsverarbeiter schriftlich informieren, damit dieser die erforderlichen Informationen bereitstellen oder dem Geschäftspartner Zugriff darauf erteilen kann.

d) Sollte es nicht möglich sein, einer gesetzlich zwingenden Auditverpflichtung anderweitig nachzukommen, können nur gesetzlich verpflichtete Parteien (z. B. eine Regulierungsbehörde, die die Aufsicht über das operative Geschäft des Geschäftspartners hat), der Geschäftspartner oder der vom Geschäftspartner beauftragte Prüfer die für die Erbringung des Services genutzten Betriebsstätten besuchen. Ein solcher Besuch ist zeitlich mit dem Auftragsverarbeiter während der üblichen Geschäftszeiten zu koordinieren, darf die Betriebsabläufe möglichst nicht stören, um Risiken für andere Geschäftspartner des Auftragsverarbeiters zu reduzieren und ist mindestens 4 Wochen voranzukündigen.

5.2 Beide Parteien tragen ihre eigenen Kosten aus Absätzen a. und b. dieses Punktes 5. Weitere Unterstützung, insbesondere aus Absätzen c. und d. stellt der Auftragsverarbeiter nach Punkt 3 bereit.

6. Rückgabe oder Löschung personenbezogener Daten des Geschäftspartners

6.1 Nach Kündigung oder Vertragsende des Hauptvertrages wird der Auftragsverarbeiter die sich in seinem Besitz befindenden personenbezogenen Daten des Geschäftspartners entweder löschen oder zurückgeben, sofern nicht durch zwingende Rechtsvorschriften etwas anderes vorgesehen ist.

6.2 Sofern nach erfolgter Rückgabe oder Löschung gemäß Punkt 6.1 weitere Verarbeitungen personenbezogener Daten des Geschäftspartners durch den Auftragsverarbeiter zur Erfüllung von nachvertraglichen Pflichten des Auftragsverarbeiters

gegenüber dem Geschäftspartner oder zur Erfüllung gesetzlicher und/oder vertraglicher Gewährleistungsansprüche des Geschäftspartners erforderlich sind, erfolgt die Verarbeitung entsprechend diesem AVV, insb. Punkt 1.4.

7. Unterauftragsverarbeiter

7.1 Der Geschäftspartner berechtigt den Auftragsverarbeiter, seinerseits weitere Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten des Geschäftspartners zu beauftragen (Unterauftragsverarbeiter). Der Auftragsverarbeiter kann die folgenden Unterauftragsverarbeiter mit Sitz im Europäischen Wirtschaftsraum für die Verarbeitung personenbezogener Daten des Geschäftspartners einsetzen:

Name des Unterauftragsverarbeiters	**Adresse, Sitz des Unterauftragsverarbeiters**
Amazon Web Services, Inc.	USA
Google LLC	USA
imgix	USA
Elasticsearch, Inc.	USA
Trello Inc.	USA
Atlassian PTY Ltd, Atlassian Inc.	USA, Großbritannien
Crazy Egg, Inc.	USA

7.2 Der Auftragsverarbeiter informiert den Geschäftspartner über jede beabsichtigte Änderung von Unterauftragsverarbeitern per E-Mail an den zuletzt gegenüber dem Auftragsverarbeiter schriftlich bekannt gegebenen Ansprechpartner des Geschäftspartners. Innerhalb eines Zeitraums von 30 Tagen nach der Benachrichtigung durch den Auftragsverarbeiter über eine beabsichtigte Änderung kann der Geschäftspartner gegen die Aufnahme eines Unterauftragsverarbeiters Einspruch erheben, wenn durch eine solche Aufnahme geltende gesetzliche Bestimmungen verletzt würden. Der Einspruch des Geschäftspartners muss schriftlich erfolgen und die Gründe des Geschäftspartners für den Einspruch sowie ggf. Kompromissmöglichkeiten beinhalten. Falls der Geschäftspartner den Unterauftragsverarbeiter innerhalb dieses Zeitraums nicht ablehnt, kann dieser mit der Verarbeitung personenbezogener Daten des Geschäftspartners beauftragt werden.

7.3 Der Auftragsverarbeiter verpflichtet sich, genehmigten Unterauftragsverarbeitern Datenschutzpflichten aufzuerlegen, die mit jenen dieser AVV und des Appendix vergleichbar sind, bevor personenbezogene Daten des Geschäftspartners durch den

Unterauftragsverarbeiter verarbeitet werden. Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Geschäftspartner erbringt.

7.4 Falls der Geschäftspartner gegen einen Unterauftragsverarbeiter rechtmäßig Einspruch erhebt und der Auftragsverarbeiter diesem Einspruch nicht Rechnung tragen kann, wird der Auftragsverarbeiter den Geschäftspartner entsprechend informieren. Der Geschäftspartner und der Auftragsverarbeiter verpflichten sich, sich über die Hinzuziehung einvernehmlich zu einigen.

8. Anfragen und Rechte betroffener Personen

8.1 Soweit gesetzlich zulässig, informiert der Auftragsverarbeiter den Geschäftspartner über Anträge von betroffenen Personen, die ihre Betroffenenrechte (z. B. Berichtigung, Löschung und Sperrung von Daten) direkt gegenüber dem Auftragsverarbeiter in Bezug auf personenbezogene Daten des Geschäftspartners geltend machen. Der Geschäftspartner ist für die Beantwortung solcher Anträge von betroffenen Personen zuständig. Der Auftragsverarbeiter unterstützt den Geschäftspartner in angemessenem Umfang bei der Beantwortung von Anträgen von betroffenen Personen gemäß Punkt 3.

8.2 Falls eine betroffene Person einen Anspruch aufgrund der Verletzung ihrer Betroffenenrechte direkt gegenüber dem Auftragsverarbeiter geltend macht, entschädigt der Geschäftspartner den Auftragsverarbeiter für sämtliche Kosten, Gebühren, Schäden, Aufwendungen oder Verluste, die sich aus einem solchen Anspruch ergeben, sofern der Auftragsverarbeiter den Geschäftspartner über den Anspruch in Kenntnis gesetzt und ihm die Möglichkeit gegeben hat, in der Abwehr und Beilegung des Anspruchs mit dem Auftragsverarbeiter zusammenzuarbeiten.

8.3 Im Rahmen der im Hauptvertrag enthaltenen Bedingungen und nach Maßgabe des Punktes 10 dieses AVV kann der Geschäftspartner vom Auftragsverarbeiter Beträge einfordern, die er an eine betroffene Person bezahlt hat, deren Betroffenenrechte durch einen schuldhaft verursachten Verstoß des Auftragsverarbeiters gegen seine Verpflichtungen aus der DSGVO verletzt wurden. Dies gilt nur, wenn er den Auftragsverarbeiter über den Anspruch in Kenntnis gesetzt und ihm die Möglichkeit gegeben hat, in der Abwehr und Beilegung des Anspruchs mit dem Geschäftspartner zusammenzuarbeiten.

9. Verletzung des Schutzes personenbezogener Daten

9.1 Der Auftragsverarbeiter wird den Geschäftspartner unverzüglich informieren, wenn der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes personenbezogener Daten in Bezug auf die Services erlangt. Der Auftragsverarbeiter wird die Verletzung des Schutzes personenbezogener Daten unverzüglich untersuchen, sofern sich diese in der Infrastruktur des Auftragsverarbeiters oder in einem anderen Bereich, für den der Auftragsverarbeiter verantwortlich ist, ereignet hat, und wird den Geschäftspartner gemäß Punkt 3 unterstützen.

10. Haftung

10.1 Der Auftragsverarbeiter erbringt seine Tätigkeiten mit größtmöglicher Sorgfalt. Die Haftung des Auftragsverarbeiters für leicht fahrlässig verursachte Schäden, der Ersatz von Folgeschäden und entgangenem Gewinn ist im weitestgehenden gesetzlich zulässigen Ausmaß ausgeschlossen. Im Übrigen ist die Haftung für in einem Vertragsjahr verursachte Schäden auf insgesamt 50% der in diesem Zeitraum verrechneten Vergütung begrenzt, wobei in jedem Fall der Geschäftspartner die Beweislast für ein haftungsbegründendes Verschulden des Auftragsverarbeiters trägt.

10.2 Schadenersatzansprüche sind vom Geschäftspartner innerhalb eines Jahres nach Kenntnis des schadensauslösenden Ereignisses und des Schädigers – spätestens aber innerhalb von drei Jahren ab Eintritt des Schadens – gerichtlich geltend zu machen, widrigenfalls sie präkludiert sind.

11. Ansprechpartner des Auftragsverarbeiters für Datenschutz

Der Geschäftspartner kann den Datenschutzansprechpartner des Auftragsverarbeiters unter datenschutz@whatchado.com kontaktieren.

12. Allgemeine Regelungen, anwendbares Recht, Gerichtsstand

12.1 Falls einzelne Regelungen dieses AVV unwirksam sind, bleiben die restlichen Regelungen davon unberührt und in vollem Umfang in Kraft. Für den Fall der Rechtsunwirksamkeit einer Bestimmung dieses AVV oder eines Vertragsteiles, gilt die unwirksame Bestimmung als durch eine solche ersetzt, die inhaltlich der unwirksamen Bestimmungen am nächsten kommt.

12.2 Soweit die Parteien zusätzliche Vereinbarungen getroffen haben, die mit diesem AVV in Widerspruch stehen, sind die Regelungen dieses AVV in Bezug auf die Verarbeitung personenbezogener Daten maßgeblich.

12.3 Für diesen AVV gilt das Recht der Republik Österreich unter Ausschluss seiner Verweisungsnormen und der Bestimmungen des UN-Kaufrechts.

12.4 **Ausschließlicher Gerichtsstand:** Zur Entscheidung aller aus diesem AVV entstehenden Streitigkeiten - einschließlich einer solchen über ihr Bestehen oder Nichtbestehen - wird die ausschließliche Zuständigkeit des sachlich zuständigen Gerichtes in Wien vereinbart.

APPENDIX

1. Verarbeitung

Der Auftragsverarbeiter wird die personenbezogenen Daten des Geschäftspartners für den Service gemäß der Beschreibung im Hauptvertrag, dem AVV und den Ergänzungen und Angaben in diesem Appendix verarbeiten.

2. Verarbeitungstätigkeiten

Der Auftragsverarbeiter führt folgende Verarbeitungstätigkeiten in Bezug auf die personenbezogenen Daten des Geschäftspartners durch:

- Kombinieren
- Kopieren
- Löschen
- Ausblenden
- Verbinden
- Unkenntlich machen
- Analysieren
- Lesen
- Aktualisieren
- Empfangen
- Senden
- Freigeben
- Speichern
- Sammeln
- Verändern
- Transformieren
- Überführen

3. Personenbezogene Daten des Geschäftspartners

3.1 Kategorien betroffener Personen

Der Auftragsverarbeiter wird die personenbezogenen Daten im Hinblick auf alle nachstehend aufgeführten Kategorien betroffener Personen in Übereinstimmung mit dem AVV und dieses Appendix verarbeiten:

- Mitarbeiterinnen und Mitarbeiter des Geschäftspartners
- potentielle Mitarbeiterinnen und Mitarbeiter des Geschäftspartners

---

Angesichts der Art des Services erkennt der Geschäftspartner an, dass der Auftragsverarbeiter die vorstehende Liste der Kategorien betroffener Personen weder überprüfen noch pflegen kann. Der Geschäftspartner wird den Auftragsverarbeiter über alle erforderlichen Änderungen an den vorstehenden Listen über die in AVV Punkt 11 genannte Kontaktmöglichkeit informieren.

Falls aufgrund solcher Änderungen an der Liste der Kategorien betroffener Personen Änderungen am vereinbarten AVV erforderlich werden, wird der Geschäftspartner den Auftragsverarbeiter ergänzende Weisungen erteilen.

3.2 Kategorien personenbezogener Daten und besondere Kategorien personenbezogener Daten

3.2.1 Kategorien personenbezogener Daten

In der folgenden Liste ist festgelegt, welche Kategorien personenbezogener Daten des Geschäftspartners der Auftragsverarbeiter im Rahmen des Service verarbeitet:

- Das Videointerview	- Das whatchado Matching	- Name	- Alter
- Geburtsort	- Geschlecht	- Herkunft, Wohnort, Standardsprache	- Arbeitsort
- Ausbildungsverhältnis	- Ausbildungs-einrichtung	- Fachrichtung	- Berufsbezeichnung bzw. Position
- Abteilung	- Arbeitgeber	- Dauer der Anstellung	- Dauer der Berufsausübung
- Akademischer Grad	- Höchste abgeschlossene Ausbildung	- E-Mail Adresse	- Sprachkenntnisse
- Wichtige Schulfächer/Kenntnisse für diesen Beruf	- Fachrichtung der höchsten abgeschlossenen Ausbildung	- Bildungseinrichtung der höchsten abgeschlossenen Ausbildung	- Stärken und Interessen; was gefällt dir an deinem Beruf und an deinem Arbeitgeber

3.2.2 Besondere Kategorien personenbezogener Daten

Es werden keine besonderen Kategorien personenbezogener Daten des Geschäftspartners im Rahmen der Service verarbeitet.

3.3 Allgemeines

Die Listen in den vorstehenden Abschnitten 3.2.1 und 3.2.2 dieses Appendix enthalten Informationen darüber, welche (besonderen) Kategorien personenbezogener Daten im Rahmen des Service generell verarbeitet werden. Der Geschäftspartner erkennt an, dass der Auftragsverarbeiter diese Listen weitgehend weder überprüfen noch pflegen kann. Der Geschäftspartner wird den Auftragsverarbeiter über alle erforderlichen Änderungen an den vorstehenden Listen über die in AVV Punkt 11 genannte Kontaktmöglichkeit informieren und wenn erforderlich ergänzende Weisungen erteilen.

4. Technische und organisatorische Maßnahmen

Der Geschäftspartner bestätigt, seiner Verpflichtung, in seinem eigenen Verantwortungsbereich geeignete technische und organisatorische Maßnahmen gemäß den Anforderungen der geltenden Datenschutzgesetze zu implementieren, nachzukommen.

Die vom Auftragsverarbeiter für den Service ergriffenen technischen und organisatorischen Maßnahmen lauten wie folgt:

4.1 Standortbezogene Maßnahmen

Der Auftragsverarbeiter hat folgende standortbezogene Maßnahmen ergriffen:

Maßnahme	***ergriffen***	***betrifft Schutzziel***			
		Vertraulich-keit	***Integrität***	***Verfüg-barkeit***	***Belast-barkeit***
Alle Standorte, an denen personenbezogene Daten des Verantwortlichen gespeichert werden, befinden sich in der EU.		**x**		**x**	
Alle Standorte, von denen aus auf personenbezogene Daten des Verantwortlichen zugegriffen werden, befinden sich entweder in der EU, in einem Drittstaat mit ausreichendem Datenschutzniveau oder sind in einem EU-Standardvertrag bzw. in genehmigten Verhaltensregeln eingebunden.		**x**		**x**	
Der Zutritt zum Gebäude, von dem heraus auf personenbezogene Daten des Verantwortlichen zugegriffen wird, ist nur befugten Personen gestattet bzw. möglich.	**x**	**x**		**x**	
Vergabe und Entzug von Zutrittsmitteln ist vollständig dokumentiert.	**x**	**x**			
Besucher, die Zutritt zum Gebäude erhalten, in dem personenbezogene Daten des Verantwortlichen verarbeitet werden, werden begleitet oder auf Vertraulichkeit verpflichtet.	**x**	**x**			
Besucher sind dazu verpflichtet, während ihres Besuches im Gebäude, in dem personenbezogene Daten des Verantwortlichen verarbeitet		**x**			

werden, einen Besucherausweis zu tragen.					
Am Standort eingesetztes Fremdpersonal (z. B. Reinigungskräfte, Sicherheitskräfte, Hausmeister) ist auf Vertraulichkeit verpflichtet worden.		**x**			
Soweit die Auftragstätigkeit für den Verantwortlichen eine Verarbeitung in einer besonderen Schutzzone erfordert, ist sichergestellt, dass für die zugehörigen Räume dieser Schutzzone besondere Zutrittsmittel nötig sind, die dazu beitragen, dass nur Befugte Zutritt zu diesen Schutzzonen erhalten.		**x**			
Soweit für die besonderen Schutzzonen darüber hinaus spezifische Vorkehrungen (wie z. B. Einbau einer Alarmanlage, Videoüberwachung, Einbruchssicherung) zu treffen sind, sind diese umgesetzt.					

4.2 Maßnahmen zum Schutz der Verarbeitungsanlage

Der Auftragsverarbeiter hat folgende verarbeitungsanlagenbezogene Maßnahmen ergriffen:

Maßnahme	***ergriffen***	***betrifft Schutzziel***			
		Vertraulich-keit	***Integrität***	***Verfüg-barkeit***	***Belast-barkeit***
Die zur Verarbeitung eingesetzten Server befinden sich in einem Serverraum, der als besondere Schutzzone behandelt wird.	**x**	**x**	**x**		
Im Serverraum, in dem sich Server befinden, mit deren Hilfe personenbezogene Daten des Verantwortlichen verarbeitet werden, befinden sich keine Wasserleitungen ohne ausreichenden Überlaufschutz und keine unnötigen Brandlasten.	**x**			**x**	
Wartungstätigkeiten durch Fremdpersonal erfolgen im Serverraum nur unter Beaufsichtigung.	**x**	**x**	**x**	**x**	
Der Serverraum verfügt über einen Mechanismus, der einen		**x**	**x**	**x**	

unbefugten Zutritt deutlich erschwert (z. B. Knauf an der Außentür, Zuzieher).					
Server, auf denen personenbezogene Daten des Verantwortlichen verarbeitet werden, und für die Verarbeitung genutzte Netzwerkkomponenten sind gehärtet, soweit dies aus funktionalen und wartungstechnischen Gründen möglich ist.		**x**	**x**	**x**	
Der Server wird nur mit personalisierten Administratoren-Accounts betrieben.	**x**	**x**	**x**	**x**	
Für den administrativen Zugang zum Server besteht ein besonderer Schutz (z. B. dedizierter Zugang, Zugang nur aus Administrationsnetzwerk, Zwei-Faktor-Authentifizierung, Transportverschlüsselung).	**x**	**x**	**x**	**x**	
Administrator-Accounts gewährleisten eine höhere Sicherheit als normale Nutzer-Accounts (z. B. durch signifikant längeres Kennwort, umfassende Kennworthistorie).	**x**	**x**	**x**	**x**	
Bei den eingesetzten Servern und zur Verarbeitung genutzten Netzwerkkomponenten wurden etwaige Standardpasswörter neu gesetzt.	**x**	**x**	**x**	**x**	
Soweit zur Administration des Servers funktionale Accounts genutzt werden, werden die Kennwörter dieser Accounts neu gesetzt, sobald ein zugangsbefugter Admin aus dem Team ausgeschieden ist.	**x**	**x**	**x**	**x**	
Auf dem Server durchgeführte Changes werden dokumentiert und wurden zuvor vom Auftragsverarbeiter sicherheitstechnisch geprüft.		**x**	**x**	**x**	
Erforderliche Sicherheitspatches werden zeitnah eingespielt.		**x**	**x**	**x**	
Für die Server besteht eine eine sichere und ausreichend robuste Default-Einstellung, um einen abgesicherten Wiederanlauf des	**x**				**x**

Serversystems in der vorgesehenen Zeit durchführen zu können.					

4.3 Maßnahmen für einen ordnungsgemäßen Betrieb

Der Auftragsverarbeiter hat folgende Maßnahmen für den laufenden Betrieb der vereinbarten Tätigkeit ergriffen:

Maßnahme	*ergriffen*	*betrifft Schutzziel*			
		Vertrau-lichkeit	*Integrität*	*Verfüg-barkeit*	*Belast-barkeit*
Für die beim Auftragsverarbeiter gespeicherten personenbezogenen Daten des Verantwortlichen besteht eine Datensicherung nach dem Stand der Technik.	**x**		**x**	**x**	**x**
Zur Datensicherung eingesetzte Medien werden im Rahmen der Archivierung getrennt von produktiven Servern, mit denen personenbezogene Daten des Verantwortlichen verarbeitet werden, aufbewahrt.	**x**			**x**	**x**
Die Wirksamkeit von Datensicherungen wird regelmäßig durch Wiedereinspieltests überprüft.				**x**	**x**
Server, auf denen personenbezogene Daten des Verantwortlichen gespeichert werden, verfügen über eine ausreichend dimensionierte unterbrechungsfreie Stromversorgung.	**x**		**x**	**x**	
Die beim Auftragsverarbeiter gespeicherten personenbezogenen Daten des Verantwortlichen werden nach Ablauf der festgelegten Speicherdauer gelöscht.	**x**	**x**			
Die zur Auftragserledigung genutzte Infrastruktur wird mit tagesaktuellen Virenscannern vor Malware geschützt.	**x**		**x**		
Beim Auftragsverarbeiter besteht eine ausreichende Netzwerksegmentierung und Netzwerksegregation.	**x**	**x**	**x**	**x**	
Die Durchführung der Auftragsarbeiten wird mindestens einmal pro Jahr hinsichtlich der Wirksamkeit getroffener Maßnahmen kontrolliert.	**x**	**x**	**x**	**x**	**x**
Wenn das Serversystem insgesamt oder für den Betrieb des Serversystems eingesetzte Komponenten ausgewechselt werden sollen, ist sichergestellt, dass sich auf zu entsorgenden Datenträgern keine	**x**	**x**			

lesbaren Daten des Verantwortlichen mehr befinden.					
Wenn Datenträger entsorgt werden sollen, die Daten des Verantwortlichen enthalten, welche mittels des eingesetzten Serversystems gespeichert, übertragen oder ausgewertet werden, werden diese Datenträger entweder physisch zerstört oder mittels einer Löschungssoftware so überschrieben, dass eine Rekonstruktion der Daten mit vertretbarem Aufwand nicht mehr möglich ist.	**x**	**x**			
Die Client-Systeme der Personen, die im Rahmen der Auftragserledigung auf personenbezogene Daten des Verantwortlichen zugreifen, weisen einen Bildschirmschutz auf, der nach ausreichend kurzer Zeit der Inaktivität, eine automatische Sperrung auslösen, die nur durch Eingabe eines Kennwortes aufgehoben werden kann.	**x**	**x**	**x**	**x**	
Benutzerpasswörter der zur Auftragserledigung eingesetzten Personen weisen eine hohe Passwortkomplexität mit mindestens acht Zeichen und unter Verwendung von Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen auf.	**x**	**x**	**x**	**x**	
Zugangsberechtigungen werden mit Ende der Gültigkeit der Berechtigungen unverzüglich gesperrt.	**x**	**x**	**x**	**x**	
Personen, die personenbezogene Daten des Verantwortlichen verarbeiten, werden über die von ihnen einzuhaltenden Pflichten informiert.	**x**	**x**	**x**	**x**	
Im laufenden Betrieb festgestellte Sicherheitsvorfälle, die personenbezogene Daten des Verantwortlichen betreffen, werden dem Verantwortlichen unverzüglich gemeldet.	**x**				**x**