Vereinbarung zur Auftragsverarbeitung

Als **Anlage zu den Allgemeinen Geschäftsbedingungen**

- nachfolgend „Leistungsvereinbarung“ -

zwischen dem

Kunden

- nachfolgend „Verantwortlicher“ -

und der **Empirio UG (haftungsbeschränkt)** (empirio)

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ –

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel

Im Rahmen der zwischen den Vertragsparteien geschlossenen Leistungsvereinbarung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Der Verantwortliche handelt als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, der Auftragsverarbeiter als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO.

Diese Vereinbarung konkretisiert die Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung personenbezogener Daten gemäß Art. 28 DSGVO sowie den einschlägigen Bestimmungen des Bundesdatenschutzgesetzes (BDSG).

Soweit anwendbar, umfassen Verweise auf die DSGVO in dieser Vereinbarung auch die britische Datenschutz-Grundverordnung („UK GDPR“) gemäß den Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 sowie den UK Data Protection Act 2018.

Soweit anwendbar, umfassen Verweise auf die DSGVO in dieser Vereinbarung auch das revidierte Schweizer Datenschutzgesetz (revDSG) sowie die hierzu erlassenen Ausführungsbestimmungen.

Soweit die Verarbeitung personenbezogene Daten von Betroffenen mit Wohnsitz in den USA oder Kanada betrifft, verpflichtet sich der Auftragsverarbeiter zusätzlich zur Einhaltung der anwendbaren Bestimmungen des California Consumer Privacy Act (CCPA) in der jeweils geltenden Fassung (inkl. CPRA) sowie des kanadischen Personal Information Protection and Electronic Documents Act (PIPEDA), sofern und soweit diese Gesetze auf die konkrete Verarbeitung Anwendung finden.

Soweit die Verarbeitung personenbezogene Daten von Betroffenen mit Wohnsitz in Australien betrifft, verpflichtet sich der Auftragsverarbeiter zusätzlich zur Einhaltung der anwendbaren Bestimmungen des Australian Privacy Act 1988 (einschließlich der Australian Privacy Principles), sofern und soweit diese Gesetze auf die konkrete Verarbeitung Anwendung finden.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

Soweit anwendbar, gilt diese Vereinbarung entsprechend für Verarbeitungen personenbezogener Daten nach der britischen Datenschutz-Grundverordnung (UK GDPR), dem revidierten Schweizer Datenschutzgesetz (revDSG), dem Australian Privacy Act sowie den US-amerikanischen (CCPA/CPRA) und kanadischen (PIPEDA) Datenschutzbestimmungen.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung. Die Allgemeinen Geschäftsbedingungen (https://www.empirio.ai/terms-of-service) stellen die Leistungsvereinbarung dar und werden bei der Registrierung durch den Verantwortlichen ausdrücklich zugestimmt.

(2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit der Leistungsvereinbarung. Die Kündigung dieser Vereinbarung entspricht einer Kündigung der Leistungsvereinbarung.

(3) Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Art der Umfragen, die Nutzung der Dienste und die Übermittlung von Daten.

(4) Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Art der Umfragen, die Nutzung der Dienste und die Übermittlung von Daten.

(5) Zur Erbringung bestimmter vertraglich vereinbarter Leistungen (z. B. automatisierte Textanalysen, Inhaltsgenerierung oder Umfrageauswertungen) setzt der Auftragsverarbeiter Systeme künstlicher Intelligenz (KI) von Drittanbietern ein. Der Auftragsverarbeiter stellt durch entsprechende vertragliche Vereinbarungen mit diesen Anbietern sicher, dass die vom Verantwortlichen übermittelten personenbezogenen Daten ausschließlich zur Erbringung der Dienstleistung verarbeitet und nicht zum Training der KI-Modelle der Drittanbieter verwendet werden.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind jeweils im Rahmen der ihnen nach den datenschutzrechtlichen Bestimmungen zugewiesenen Verantwortlichkeiten für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter ist, falls dies unter Berücksichtigung der Schwere des Verstoßes erforderlich ist, berechtigt, die Verarbeitung auszusetzen oder die Leistungsvereinbarung außerordentlich zu kündigen.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) Die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen erfolgt grundsätzlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums. Eine Verarbeitung in Staaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Drittländer) ist zulässig, sofern die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Dies gilt insbesondere, wenn

a) für das betreffende Drittland ein Angemessenheitsbeschluss der Europäischen Kommission besteht, oder

b) geeignete Garantien im Sinne des Art. 46 DSGVO vorgesehen sind, insbesondere durch den Abschluss der von der Europäischen Kommission erlassenen Standardvertragsklauseln.

Soweit für eine Übermittlung kein Angemessenheitsbeschluss besteht und stattdessen geeignete Garantien nach Art. 46 DSGVO eingesetzt werden, werden die Standardvertragsklauseln – sofern das Datenschutzrecht des Vereinigten Königreichs (UK GDPR) Anwendung findet – zusätzlich in der jeweils erforderlichen Fassung nach UK-Recht ergänzt (insbesondere UK International Data Transfer Addendum oder International Data Transfer Agreement). Soweit das Schweizer revDSG Anwendung findet, werden die Standardvertragsklauseln mit den erforderlichen Anpassungen nach Schweizer Recht ergänzt (Schweizer Addendum).

Die Verarbeitung personenbezogener Daten in der Schweiz, im Vereinigten Königreich sowie für kommerzielle Organisationen in Kanada (PIPEDA) gilt als Verarbeitung in einem Drittland mit angemessenem Datenschutzniveau im Sinne eines Angemessenheitsbeschlusses.

Der Einsatz von Unterauftragsverarbeitern in Drittländern ist im Anhang 2 zu dieser Vereinbarung aufgeführt. Der Verantwortliche erteilt hiermit seine allgemeine Genehmigung zur Beauftragung der dort genannten Unterauftragsverarbeiter. § 8 dieser Vereinbarung bleibt unberührt.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen Festlegung angemessener technischer und organisatorischer Maßnahmen für die jeweilige Verarbeitungssituation.

(10) Besondere Bestimmungen für international Betroffene:
1. Der Auftragsverarbeiter agiert als „Service Provider“ im Sinne des CCPA/CPRA (USA) sowie vergleichbarer Bestimmungen des PIPEDA (Kanada) und des Australian Privacy Act. Er wird personenbezogene Daten nicht verkaufen oder über den geschäftlichen Zweck hinaus teilen.
2. Soweit die Verarbeitung Betroffene in Kanada, Australien, dem Vereinigten Königreich (UK GDPR) oder der Schweiz (revDSG) betrifft, garantiert der Auftragsverarbeiter die Einhaltung der jeweiligen lokalen Datenschutzrechte, insbesondere in Bezug auf Auskunft, Berichtigung und Löschung.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO).

(3) Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, die/der ihre/seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten der/des Datenschutzbeauftragten sind: Empirio UG (haftungsbeschränkt), Datenschutzbeauftragter, 31785 Hameln, info@empirio.ai.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang 1 „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind.

(4) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, die er für die Prüfung für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten benötigt und hilft den Verantwortlichen bei einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO mit den ihm zur Verfügung stehenden Mitteln. Die Bereitstellung von Informationen erfolgt nur insoweit, als der Verantwortliche diese sich nicht selbst beschaffen kann.

(5) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchfuhren.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Löschung des Kontos oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung wird dem Verantwortlichen auf Anforderung bestätigt.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungs- fristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2. Der Auftragsverarbeiter bewahrt personenbezogene Daten auch in aggregierter Form für statistische Zwecke auf, sofern diese Daten angemessenen Garantien unterliegen, insbesondere im Einklang mit den Art. 5 Abs. 1 lit. b, Art. 14 Abs. 5 lit. b, Art. 17 Abs. 3 lit. d, Art. 21 Abs. 6 und Art. 89 DSGVO stehen.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter (Subunternehmen) zur Erfüllung der vertraglich geschuldeten Leistungen einzusetzen. Der Verantwortliche erteilt hiermit seine allgemeine Genehmigung zur Beauftragung von Subunternehmen im Sinne des Art. 28 Abs. 2 DSGVO. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subunternehmen sind in Anhang 2 zu dieser Vereinbarung aufgeführt. Der Auftragsverarbeiter wird den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Subunternehmen rechtzeitig informieren.

(2) Der Verantwortliche ist berechtigt, aus wichtigem datenschutzrechtlichem Grund gegen die Beauftragung eines neuen oder ersetzten Subunternehmens Widerspruch zu erheben. Der Widerspruch ist innerhalb von 14 Tagen nach Zugang der Mitteilung in Textform zu erklären. Legt der Verantwortliche fristgerecht Widerspruch ein und ist dem Auftragsverarbeiter ein Festhalten an der Beauftragung des Subunternehmens nicht zumutbar, sind beide Vertragsparteien berechtigt, die Leistungsvereinbarung außerordentlich zu kündigen.

(3) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, jährlich auf Anforderung des Verantwortlichen die erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 5 dieser Vereinbarung dokumentenbasiert zur Verfügung zu stellen, soweit der Verantwortliche sich diese nicht selbst beschaffen kann und sie dem Auftragsverarbeiter vorliegen. Der Verantwortliche kann hierfür Dokumentationen, Zertifizierungen und Testate einholen. Die durch diese Kontrolle verursachten Aufwände werden mit einem Stundensatz von 90€ angesetzt und ist vom Verantwortlichen zu tragen. Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Sollte eine Aufsichtsbehörde den Auftragsverarbeiter aufgrund schuldhaften Verhaltens des Verantwortlichen kontrollieren, ist der hierfür anfallende Personal- und Materialaufwand vom Verantwortlichen zu tragen.

§ 10 Schlussbestimmungen

(1) Der Auftragsverarbeiter kann Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile mit einer Vorlaufsfrist von zwei Wochen ändern oder ersetzen. Auf Änderungen oder Ersetzungen der Vereinbarung wird der Verantwortliche per E-Mail oder in seinem Account hingewiesen. Dem Verantwortlichen steht ein außerordentliches Kündigungsrecht zu, welches er innerhalb 30 Tage ab Hinweis ausüben kann.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

(3) Es gilt deutsches Recht.

(4) Diese Vereinbarung ist in deutscher und englischer Sprache verfügbar. Im Falle von Abweichungen oder Auslegungsfragen ist die deutsche Fassung maßgeblich. Die englische Fassung dient lediglich der Information.

Anhang 1 „Technisch-organisatorische Maßnahmen“

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten o- der Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Maßnahme	**Umsetzung der Maßnahme**
Zutrittskontrolle Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	Zutrittskontrollsystem zu Büroräumen, Lagerung von vertraulichen Dokumenten unter Verschluss in abschließbaren Schränken.
Zugangskontrolle Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Verwendung von dem aktuellen Stand der Technik, Regelmäßiger Passwortwechsel, Passwortschutz für Systeme, Zweifaktor-Authentifizierung bei personenbezogenen Daten, Verschlüsselungsverfahren.
Zugriffskontrolle Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Berechtigungskonzept mit definierten Rechten & Rollen, automatisierte Überwachungen der Zugriffe.

Weitergabekontrolle Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	SSL-Verschlüsselung, Firewall, Virenschutz, AV-Vertrag, Passwortschutz von einzelnen Dokumenten, VPN Tunnel.
Eingabekontrolle Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Interne Historisierung und Protokollierung von Änderungen.
Auftragskontrolle Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	Abgrenzung der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter durch eindeutige Vertragsgestaltung mit Abgrenzung der Verantwortlichkeiten zwischen Verantwortlichem und Auftragsverarbeiter, Bestellung eines Datenschutzbeauftragten.
Verfügbarkeitskontrolle Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Tägliche Backup-Verfahren, Firewall & Virenschutz, Notfallplan, SLA-Vereinbarungen bei den Unterauftragnehmern.
Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Funktionstrennung zwischen Produktion und Test, In der Entwicklung werden nur Testdaten verwendet.

Die technischen und organisatorischen Maßnahmen werden regelmäßig überprüft und bei Bedarf an den Stand der Technik angepasst, ohne dass hierdurch das vereinbarte Sicherheitsniveau unterschritten wird.

Anhang 2 – „Unterauftragsverhältnisse und Drittlandverarbeitung“

§ 3 und § 8 der Vereinbarung zur Auftragsverarbeitung verweisen zur Konkretisierung der Unterauftragnehmer auf diesen Anhang. Die nachfolgend aufgeführten Unterauftragsverarbeiter werden zur Erbringung der vertraglich geschuldeten Leistungen eingesetzt. Soweit eine Verarbeitung personenbezogener Daten in einem Drittland erfolgt, geschieht dies unter Einhaltung der Anforderungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage geeigneter Garantien im Sinne des Art. 46 DSGVO.

- **Lebenslauf.de GmbH**; Deisterstraße 20, 31785 Hameln, Deutschland
  - **Leistung:** Hosting, Betrieb der Software
  - **Datenverarbeitung:** Europäische Union
- **Synatix GmbH**; Deisterstraße 20, 31785 Hameln, Deutschland
  - **Leistung:** Hosting, Betrieb der Software
  - **Datenverarbeitung:** Europäische Union
- **Sendinblue GmbH (Brevo)**; Köpenicker Straße 126, 10179 Berlin, Deutschland
  - **Leistung:** Versand von Marketing-E-Mails
  - **Datenverarbeitung:** Europäische Union
- **METAVISION GmbH**; Untere Bachgasse 15, 93047 Regensburg, Deutschland
  - **Leistung:** Hosting und Betriebsaufgaben
  - **Datenverarbeitung:** Europäische Union
- **Supabase, Inc., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513**
  - **Leistung**: Hosting/DB/Auth/Storage/Operations
  - **Übermittlungsgrundlage**: Art. 46 DSGVO (SCC) bzw. Angemessenheitsbeschlüsse, je nach Konstellation
  - **Datenverarbeitung**: Europäische Union (Datenbank) / Singapur (Administration & Metadaten)
- **Amazon Web Services EMEA SARL**; 38 Avenue John F. Kennedy, L-1855 Luxemburg
  - **Leistung:** Hosting und Betriebsaufgaben
  - **Übermittlungsgrundlage:** Geeignete Garantien gemäß Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln) sowie ggf. das EU-U.S. Data Privacy Framework
  - **Datenverarbeitung:** Europäische Union
- **Vercel Inc.**; 440 N Barranca Ave #4133, Covina, CA 91723, USA
  - **Leistung:** Hosting und Betriebsaufgaben
  - **Übermittlungsgrundlage:** Geeignete Garantien gemäß Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln) sowie ggf. das EU-U.S. Data Privacy Framework
  - **Datenverarbeitung:** USA / Europäische Union (Edge Network)
- **Groq, Inc.**; 2700 Zanker Road, Suite 150, San Jose, CA 95134, USA
  - **Leistung:** Bereitstellung von KI-Tools
  - **Übermittlungsgrundlage:** Geeignete Garantien gemäß Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln) sowie ggf. das EU-U.S. Data Privacy Framework
  - **Datenverarbeitung:** USA
- **OpenAI OpCo, LLC.**; 1455 3rd Street, San Francisco, CA 94158, USA
  - **Leistung:** Bereitstellung von KI-Tools

- **Übermittlungsgrundlage:** Geeignete Garantien gemäß Art. 46 DSGVO (insbesondere EU-Standardvertragsklauseln) sowie ggf. das EU-U.S. Data Privacy Framework
- **Datenverarbeitung:** USA