



AIDERA-Datenverarbeitungsvereinbarung

Vereinbarung über die Verarbeitung personenbezogener Daten

zwischen

Aidera GmbH, Leopoldstraße 20, 80802 München,

– im Folgenden („Auftragsverarbeiter“) –

und

dem Kunden (im Folgenden „Kunde“)

Der Auftragsverarbeiter und der Kunde (im Folgenden zusammen „Parteien“ und einzeln „Partei“) schließen die folgende Vereinbarung über die Verarbeitung personenbezogener Daten (Datenverarbeitungsvereinbarung, „DPA“) durch den Auftragsverarbeiter im Auftrag des Kunden gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, „DSGVO“).

1. PRÄAMBEL

Der Auftragsverarbeiter bietet dem Kunden die Bereitstellung des vertraglichen AIDERA SaaS-Angebots („Dienst“) an, wie in der zugrunde liegenden SaaS-Vereinbarung („**Hauptvereinbarung**“) näher beschrieben und spezifiziert.

Im Rahmen der Ausführung des Hauptvertrags stellt der Kunde (als Datenverantwortlicher) dem Auftragsverarbeiter personenbezogene Daten („**personenbezogene Daten des Kunden**“) zur Verfügung, die der Auftragsverarbeiter im Auftrag des Kunden verarbeitet.

Wenn in dieser DPA Begriffe verwendet werden, die in der DSGVO definiert sind, haben diese Begriffe die ihnen in der DSGVO zugewiesene Bedeutung.

2. GEGENSTAND UND GELTUNGSBEREICH DER DPA

- 2.1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten des Kunden im Auftrag und gemäß den Anweisungen des Kunden (Auftragsverarbeitung). Der Kunde bleibt der Datenverantwortliche.
- 2.2. Der Umfang, die Art und Weise und der Zweck der Verarbeitung der personenbezogenen Daten des Kunden durch den Auftragsverarbeiter sind in der Hauptvereinbarung und in Anhang 1 dieser DPA festgelegt; die Verarbeitung bezieht sich auf die darin angegebenen Arten von personenbezogenen Daten des Kunden und Kategorien von betroffenen Personen. Die personenbezogenen Daten des Kunden umfassen im Allgemeinen keine besonderen Kategorien personenbezogener Daten des Kunden im Sinne von Art. 9 Abs. 1 DSGVO.
- 2.3. Die Parteien schließen diese DPA, um die gegenseitigen Rechte und Pflichten gemäß der DSGVO festzulegen. Im Zweifelsfall haben die Bestimmungen dieser DPA Vorrang vor den Bestimmungen des Hauptvertrags, soweit es um die Verarbeitung der personenbezogenen Daten des Kunden geht.
- 2.4. Die Verarbeitung der personenbezogenen Daten des Kunden durch den Auftragsverarbeiter erfolgt grundsätzlich innerhalb der Europäischen Union oder eines anderen Vertragsstaates des Europäischen Wirtschaftsraums („EWR“). Der Auftragsverarbeiter ist jedoch berechtigt, personenbezogene Daten des Kunden gemäß den Bestimmungen dieser DPA außerhalb des EWR zu



verarbeiten, wenn der Auftragsverarbeiter den Kunden mit dieser DPA und anderweitig im Voraus über den Ort der Verarbeitung informiert und wenn die Anforderungen der Art. 44 bis 48 DSGVO erfüllt sind oder wenn eine Ausnahme gemäß Art. 49 DSGVO gilt.

- 2.5. Die gesamte Kommunikation zwischen den Parteien kann in Textform erfolgen, einschließlich, aber nicht beschränkt auf E-Mail. Im Namen beider Parteien sind nur bevollmächtigte Personen berechtigt, Mitteilungen oder Anweisungen zu erteilen oder entgegenzunehmen sowie Anfragen zu stellen und zu beantworten, sofern zwischen den Parteien nichts anderes vereinbart wurde.

3. PFLICHTEN DES KUNDEN

- 3.1. Der Kunde ist als Verantwortlicher allein verantwortlich für die Beurteilung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten des Kunden und für die Wahrung der Rechte der betroffenen Personen im Verhältnis zwischen den Parteien.
- 3.2. Auf Anfrage stellt der Kunde dem Auftragsverarbeiter die in Art. 30 Abs. 2 DSGVO genannten Informationen zur Verfügung, soweit diese dem Auftragsverarbeiter nicht selbst zur Verfügung stehen.
- 3.3. Wenn der Auftragsverarbeiter verpflichtet ist, einer staatlichen Stelle oder Person Informationen über die Verarbeitung der personenbezogenen Daten des Kunden zur Verfügung zu stellen oder in anderer Weise mit diesen Stellen zusammenzuarbeiten, ist der Kunde verpflichtet, den Auftragsverarbeiter auf erste Aufforderung hin bei der Bereitstellung dieser Informationen und der Erfüllung anderer Kooperationspflichten zu unterstützen.

4. RECHT AUF WEISUNGEN

- 4.1. Der Auftragsverarbeiter darf die personenbezogenen Daten des Kunden nur im Rahmen des Hauptvertrags, dieser DPA und gemäß den Anweisungen des Kunden verarbeiten. Ist der Auftragsverarbeiter aufgrund der Rechtsvorschriften der Europäischen Union oder der Mitgliedstaaten, denen er unterliegt, zur weiteren Verarbeitung der personenbezogenen Daten des Kunden verpflichtet, so hat er den Kunden vor der Verarbeitung über diese gesetzlichen Anforderungen zu informieren, soweit dies gesetzlich zulässig ist.
- 4.2. Die Weisungen des Kunden sind zunächst im Hauptvertrag und in dieser DPA festgelegt und können anschließend vom Kunden in Textform durch spezifische Weisungen (Einzelweisungen) geändert, ergänzt oder ersetzt werden. Der Kunde ist berechtigt, jederzeit entsprechende Anweisungen zu erteilen. Dazu gehören Anweisungen zur Berichtigung und Löschung der personenbezogenen Daten des Kunden sowie zur Einschränkung der Verarbeitung. Im Namen beider Parteien sind nur bevollmächtigte Personen berechtigt, Anweisungen zu erteilen oder entgegenzunehmen, sofern zwischen den Parteien nichts anderes vereinbart wurde.
- 4.3. Alle erteilten Anweisungen müssen sowohl vom Kunden als auch vom Auftragsverarbeiter in Textform dokumentiert werden. Anweisungen, die über die im Hauptvertrag vereinbarte Dienstleistung hinausgehen, werden als Antrag auf eine Änderung der Dienstleistung behandelt und unterliegen der jeweiligen Änderungsmanagementregelung im Hauptvertrag oder, falls keine spezifische Änderungsmanagementregelung vereinbart wurde, einer neuen Vereinbarung.
- 4.4. Ist der Auftragsverarbeiter der Ansicht, dass eine Anweisung des Kunden gegen diese DPA oder geltende Datenschutzbestimmungen verstößt, wird er den Kunden unverzüglich darüber informieren. Der Auftragsverarbeiter ist berechtigt, die Ausführung der betreffenden Anweisung auszusetzen, bis sie vom Kunden bestätigt oder geändert wird.

5. SCHUTZMAßNAHMEN DES AUFTRAGSVERARBEITERS

- 5.1. In seinem Verantwortungsbereich gestaltet der Auftragsverarbeiter seine interne Organisation so, dass sie den Anforderungen der geltenden Datenschutzgesetze entspricht. Der Auftragsverarbeiter



ist verpflichtet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung der personenbezogenen Daten des Kunden sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen zu ergreifen, insbesondere die in Anhang 2 aufgeführten Maßnahmen, und diese für die Dauer dieser DPA aufrechtzuerhalten.

- 5.2. Die technischen und organisatorischen Maßnahmen können an zukünftige technologische Entwicklungen angepasst werden. Die angepassten Maßnahmen müssen mindestens dem Sicherheitsniveau der in Anhang 2 vereinbarten Maßnahmen entsprechen.
- 5.3. Den Mitarbeitern des Auftragsverarbeiters ist es untersagt, personenbezogene Daten des Kunden ohne Genehmigung zu verarbeiten. Der Auftragsverarbeiter verpflichtet alle Personen, die mit der Verarbeitung personenbezogener Daten des Kunden und der Erfüllung dieser DPA befasst sind, entsprechend und weist sie über die besonderen Datenschutzverpflichtungen aus dieser DPA und die bestehenden Weisungen und Zweckbindung hin. Der Auftragsverarbeiter verpflichtet alle Personen, die mit der Verarbeitung personenbezogener Daten des Kunden befasst sind, zur Vertraulichkeit hinsichtlich der Verarbeitung personenbezogener Daten des Kunden.

6. ANFRAGEN UND RECHTE DER BETROFFENEN PERSONEN

- 6.1. Der Auftragsverarbeiter unterstützt den Kunden in angemessenem und erforderlichem Umfang mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Verpflichtungen des Kunden gemäß Art. 12 bis 22 DSGVO gegen Erstattung der dem Auftragsverarbeiter dadurch entstehenden zusätzlichen Aufwendungen und Kosten.
- 6.2. Wenn eine betroffene Person Rechte wie das Recht auf Auskunft, Berichtigung oder Löschung ihrer personenbezogenen Daten direkt gegenüber dem Auftragsverarbeiter geltend macht, wird der Auftragsverarbeiter nicht selbstständig reagieren, sondern die betroffene Person unverzüglich an den Kunden verweisen und dessen Anweisungen abwarten.

7. UNTERSTÜTZUNGS- UND BENACHRICHTIGUNGSPFLICHTEN DES AUFTRAGSVERARBEITERS

- 7.1. Der Auftragsverarbeiter unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Verpflichtungen gemäß Art. 32 DSGVO.
- 7.2. Soweit der Kunde aufgrund einer Verletzung der Sicherheit seiner personenbezogenen Daten einer gesetzlichen Meldepflicht unterliegt (insbesondere gemäß Art. 33, 34 DSGVO), informiert der Auftragsverarbeiter den Kunden unverzüglich über alle meldepflichtigen Vorfälle in seinem Verantwortungsbereich. Der Auftragsverarbeiter unterstützt den Kunden auf dessen Wunsch bei der Erfüllung der Meldepflichten, soweit dies angemessen und erforderlich ist, gegen Erstattung der ihm dadurch entstehenden zusätzlichen Aufwendungen und Kosten.
- 7.3. Der Auftragsverarbeiter unterstützt den Kunden in angemessenem und erforderlichem Umfang gegen Erstattung der ihm dadurch entstehenden zusätzlichen Aufwendungen und Kosten bei der Durchführung von Datenschutz-Folgenabschätzungen durch den Kunden und gegebenenfalls bei anschließenden Konsultationen mit der Aufsichtsbehörde gemäß Art. 35, 36 DSGVO.

8. KONTROLLRECHTE DES KUNDEN

- 8.1. Der Auftragsverarbeiter stellt dem Kunden auf dessen Anfrage alle erforderlichen und ihm zur Verfügung stehenden Informationen zur Verfügung, um die Einhaltung seiner Verpflichtungen aus dieser DPA nachzuweisen.



- 8.2. Der Kunde ist berechtigt, den Auftragsverarbeiter hinsichtlich der Einhaltung der Bestimmungen dieser DPA, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen, einschließlich Inspektionen.
- 8.3. Der Kunde führt Inspektionen nur im erforderlichen Umfang und gegen Erstattung der zusätzlichen Kosten und Aufwendungen durch. Inspektionen dürfen die Betriebsabläufe des Auftragsverarbeiters nicht unverhältnismäßig stören. Nach rechtzeitiger Vorankündigung gemäß Abschnitt „8.4 “ dieser DPA ist der Kunde berechtigt, zur Durchführung von Inspektionen auf eigene Kosten die Geschäftsräume des Auftragsverarbeiters, in denen die personenbezogenen Daten des Kunden verarbeitet werden, innerhalb der üblichen Geschäftszeiten (montags bis freitags von 9 bis 17 Uhr) zu betreten, ohne den Geschäftsbetrieb zu stören und unter strikter Wahrung der Geschäfts- und Betriebsgeheimnisse des Auftragsverarbeiters.
- 8.4. Der Kunde hat den Auftragsverarbeiter mindestens vier Wochen im Voraus über alle Umstände im Zusammenhang mit der Durchführung des Audits zu informieren. Der Kunde kann pro Kalenderjahr ein Audit durchführen. Diese Regelung gilt nicht für Audits nach einem Sicherheitsvorfall, der die Anforderungen von Art. 33 DSGVO oder Art. 34 DSGVO erfüllt.
- 8.5. Der Auftragsverarbeiter ist berechtigt, nach eigenem Ermessen und unter Berücksichtigung der gesetzlichen Verpflichtungen des Kunden keine Informationen offenzulegen, die für das Geschäft des Auftragsverarbeiters sensibel sind oder wenn der Auftragsverarbeiter durch deren Offenlegung gegen gesetzliche oder andere vertragliche Bestimmungen verstoßen würde. Der Kunde ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragsverarbeiters, Kosteninformationen, Berichten zur Qualitätskontrolle und zum Vertragsmanagement oder anderen vertraulichen Daten des Auftragsverarbeiters zu erhalten, die für die vereinbarten Audit-Zwecke nicht unmittelbar relevant sind.
- 8.6. Beauftragt der Kunde einen Dritten mit der Durchführung des Audits, so verpflichtet er diesen Dritten schriftlich in gleicher Weise, wie er selbst gegenüber dem Auftragsverarbeiter gemäß diesem Abschnitt der DPA verpflichtet ist. Darüber hinaus verpflichtet der Kunde den Dritten zur Geheimhaltung und Vertraulichkeit, es sei denn, der Dritte unterliegt einer beruflichen Geheimhaltungspflicht. Auf Verlangen des Auftragsverarbeiters legt der Kunde dem Auftragsverarbeiter unverzüglich eine Kopie der Verpflichtungsvereinbarung mit dem Dritten vor. Der Kunde darf keinen Wettbewerber des Auftragsverarbeiters mit der Durchführung des Audits beauftragen.
- 8.7. Der Kunde dokumentiert die Ergebnisse der von ihm durchgeführten oder in Auftrag gegebenen Audits und informiert den Auftragsverarbeiter über deren Ergebnis. Stellt der Kunde bei der Prüfung Fehler oder Unregelmäßigkeiten fest, muss er den Auftragsverarbeiter unverzüglich darüber informieren. Werden bei der Prüfung Sachverhalte festgestellt, die Änderungen des bestellten Verfahrens erfordern, um solche Sachverhalte in Zukunft zu vermeiden, informiert der Kunde den Auftragsverarbeiter unverzüglich über die erforderlichen Verfahrensänderungen.
- 8.8. Nach Ermessen des Auftragsverarbeiters kann der Nachweis der Einhaltung der Verpflichtungen aus dieser DPA anstelle einer Prüfung durch Vorlage eines entsprechenden aktuellen Gutachtens oder Berichts einer unabhängigen Stelle (z. B. Wirtschaftsprüfer, Revisionsstelle, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzprüfer oder Qualitätsprüfer) oder einer geeigneten Zertifizierung durch eine IT-Sicherheits- oder Datenschutzprüfung – z. B. gemäß BSI-Grundschutz, wenn der Auditbericht es dem Kunden in geeigneter Weise ermöglicht, sich von der Einhaltung der vertraglichen Verpflichtungen zu überzeugen, sofern nicht durch geltende gesetzliche Vorschriften etwas anderes bestimmt ist.

9. EINSATZ VON UNTERAUFTRAGSVERARBEITERN

- 9.1. Der Kunde erteilt dem Auftragsverarbeiter eine allgemeine Ermächtigung, weitere Unterauftragsverarbeiter mit der Verarbeitung der personenbezogenen Daten des Kunden zu beauftragen. Die in Anhang 3 aufgeführten Unterauftragsverarbeiter sind vom Kunden autorisiert. Der Auftragsverarbeiter ist berechtigt, im Rahmen seiner vertraglichen Verpflichtungen weitere



Unterauftragsverhältnisse mit Unterauftragsverarbeitern einzugehen. Der Auftragsverarbeiter ist verpflichtet, Unterauftragsverarbeiter sorgfältig nach ihrer Eignung und Zuverlässigkeit auszuwählen.

- 9.2. Der Auftragsverarbeiter hat den Kunden über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder den Austausch von Unterauftragsverarbeitern zu informieren. In Einzelfällen hat der Kunde das Recht, der Beauftragung eines potenziellen Unterauftragsverarbeiters zu widersprechen. Ein Widerspruch kann vom Kunden nur aus wichtigen Gründen erhoben werden, die näher zu erläutern sind. Sofern der Kunde nicht innerhalb von vierzehn (14) Tagen nach Erhalt der Mitteilung schriftlich Widerspruch einlegt, erlischt sein Recht, der entsprechenden Beauftragung zu widersprechen. Legt der Kunde Widerspruch ein, ist der Auftragsverarbeiter berechtigt, den Hauptvertrag und diese DPA mit einer Frist von drei Monaten zu kündigen.
- 9.3. Die Vereinbarung zwischen dem Auftragsverarbeiter und dem weiteren Unterauftragsverarbeiter muss diesem im Wesentlichen die gleichen Verpflichtungen auferlegen, wie sie dem Auftragsverarbeiter gemäß dieser DPA obliegen. Die Parteien sind sich einig, dass diese Anforderung erfüllt ist, wenn der Vertrag ein Schutzniveau aufweist, das dieser DPA entspricht.
- 9.4. Vorbehaltlich der Einhaltung der Anforderungen des Abschnitts 2.4 dieser DPA gelten die Bestimmungen dieses Abschnitts auch, wenn ein Unterauftragsverarbeiter in einem Drittland beteiligt ist. Die Parteien sind sich einig, dass in einem solchen Fall die Anforderungen des vorstehenden Abschnitts 9.3 erfüllt sind, wenn die geltenden EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer mit dem weiteren Auftragsverarbeiter im Drittland vereinbart wurden. Der Kunde erklärt sich bereit, bei der Erfüllung der Anforderungen des Art. 49 DSGVO im erforderlichen Umfang mitzuwirken.
- 9.5. Die Beauftragung Dritter mit Dienstleistungen, die vom Auftragsverarbeiter als reine Nebenleistungen anzusehen sind, begründet kein Unterauftragsverhältnis im Sinne dieser Bestimmungen. Dazu gehören beispielsweise Post-, Transport- und Versanddienstleistungen, Reinigungsdienstleistungen, Telekommunikationsdienstleistungen ohne konkreten Bezug zu den Dienstleistungen, die der Auftragsverarbeiter für den Kunden erbringt, sowie Sicherheitsdienstleistungen und sonstige Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungssystemen. Die Verpflichtung des Auftragsverarbeiters zur Gewährleistung der Einhaltung des Datenschutzes und der Datensicherheit bleibt in diesen Fällen unberührt.

10. HAFTUNG

- 10.1. Es gelten die Haftungsbeschränkungen des Hauptvertrags.
- 10.2. Soweit Dritte Ansprüche gegen den Auftragsverarbeiter geltend machen, die durch einen schuldhaften Verstoß des Kunden gegen diese DPA oder eine seiner Verpflichtungen als Verantwortlicher im Sinne der DSGVO verursacht wurden, stellt der Kunde den Auftragsverarbeiter von diesen Ansprüchen frei und hält ihn schadlos.
- 10.3. Der Kunde verpflichtet sich, den Auftragsverarbeiter von allen möglichen Geldbußen freizustellen, die gegen den Auftragsverarbeiter verhängt werden und dem Anteil des Kunden an der Verantwortung für den mit der Geldbuße sanktionierten Verstoß entsprechen.

11. LAUFZEIT UND KÜNDIGUNG

- 11.1. Die Laufzeit dieser DPA richtet sich nach der Laufzeit des Hauptvertrags, sofern die Umstände dieser DPA nichts anderes erfordern.
- 11.2. Die Kündigung dieser DPA richtet sich nach den entsprechenden Bestimmungen des Hauptvertrags. Eine Kündigung des Hauptvertrags führt automatisch zur Aufhebung dieser DPA. Eine isolierte Kündigung dieser DPA ist ausgeschlossen.



12. LÖSCHUNG DER PERSONENBEZOGENEN DATEN DES KUNDEN

Nach Beendigung des Hauptvertrags oder jederzeit auf schriftliche Anfrage des Kunden (Textform genügt) löscht der Auftragsverarbeiter alle ihm zur Verfügung gestellten personenbezogenen Daten des Kunden, es sei denn, der Auftragsverarbeiter ist gesetzlich zur weiteren Speicherung der personenbezogenen Daten des Kunden verpflichtet.

13. SCHLUSSBESTIMMUNGEN

- 13.1. Sollten einzelne Bestimmungen dieser DPA unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen davon unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine rechtlich zulässige Bestimmung zu ersetzen, die dem Zweck der unwirksamen Bestimmung am nächsten kommt und damit den Anforderungen des Art. 28 DSGVO entspricht.
- 13.2. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit der DPA ist München, Deutschland. Der Auftragsverarbeiter ist auch berechtigt, am Sitz des Kunden oder einem anderen zuständigen Gericht zu klagen.
- 13.3. Es gilt das Recht der Bundesrepublik Deutschland.

Anhänge zu dieser DPA

Anhang 1: Beschreibung der Datenarten und Kategorien der betroffenen Personen

Anhang 2: Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Anhang 3: Autorisierte Unterauftragsverarbeiter

ANHANG 1: BESCHREIBUNG DER ARTEN VON DATEN UND KATEGORIEN VON BETROFFENEN PERSONEN

Betroffene Personen und Personengruppen	Insbesondere: • Kunden des Kunden oder andere Geschäftspartner des Kunden • Mitarbeiter des Kunden, einschließlich Freiberufler und Mitarbeiter weiterer vom Kunden beauftragter Auftragnehmer
Art der Daten oder Datenkategorien	Insbesondere: • Kontodaten (z. B. Name, geschäftliche E-Mail-Adresse, Anschrift, IP-Adresse, Telefonnummer) • Geschäftliche Kontaktdaten der Mitarbeiter des Kunden (z. B. Name, geschäftliche E-Mail-Adresse, geschäftliche Telefonnummer) • Geschäftliche Kontaktdaten der Kunden des Kunden und anderer Geschäftspartner (z. B. Name, geschäftliche E-Mail-Adresse, geschäftliche Telefonnummer) • Zugriffs- und Nutzungsdaten in Bezug auf den Dienst (z. B. IP-Adressen, Anmeldeinformationen, Gerätedaten) • Kundeneinhaltsdaten (z. B. technische Zeichnungen, statistische Daten, Preisdaten, Qualitätsberichte, Beschreibungen, Listen oder andere kundenspezifische Daten)
Art und Zweck der Verarbeitung	• Erhebung, Verwendung, Speicherung und Löschung personenbezogener Daten • Erbringung von Supportleistungen für den Kunden • Erbringung der Dienstleistungen des Auftragsverarbeiters über den Dienst





ANHANG 2: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN DES AUFTRAGSVERARBEITERS

LISTE DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

§ 1 VERTRAULICHKEIT GEMÄß ART. 32 ABS. 1 DSGVO

Aidera ergreift die folgenden technischen und organisatorischen Maßnahmen zur Datensicherheit gemäß Art. 32 DSGVO.

Aidera betreibt ein risikobasiertes Informationssicherheits- und Datenschutzmanagementsystem. Die Maßnahmen konzentrieren sich auf Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit. Alle Maßnahmen werden mindestens einmal jährlich überprüft und bei Bedarf angepasst.

Maßnahmen zur Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 Buchstabe b DSGVO)

Physische Zugangskontrolle

Maßnahmen, die verhindern sollen, dass Unbefugte Zugang zu Datenverarbeitungsanlagen erhalten, in denen personenbezogene Daten verarbeitet oder genutzt werden.

Die Geschäftsräume der Aidera GmbH befinden sich in der Leopoldstraße 20, 80802 München. Eine Speicherung oder Verarbeitung personenbezogener Daten der Produktion findet am Standort der Geschäftsräume nicht statt.

- Wichtige Managementrichtlinien
- Sorgfältige Auswahl und Überprüfung des Reinigungspersonals
- Besucher werden stets von Mitarbeitern begleitet

Die Produktionsverarbeitung erfolgt ausschließlich in EU/EWR-Cloud-Regionen der etablierten und geprüften Unterauftragsverarbeiter. Die Sicherheits- und Datenverarbeitungsdokumentation der Unterauftragsverarbeiter, einschließlich anerkannter Zertifizierungen wie SOC 2 oder ISO 27001, ist unter den oben aufgeführten Referenzen öffentlich zugänglich, wie in der vollständigen Liste der Unterauftragsverarbeiter in Anhang 3 unten aufgeführt.

Systemzugriffskontrolle

Maßnahmen, die verhindern sollen, dass Datenverarbeitungssysteme von unbefugten Personen genutzt werden.

- Obligatorische MFA für alle Verwaltungs- und Produktionszugriffe
- Zentralisiertes IAM mit rollenbasierter Zugriffskontrolle nach dem Prinzip der geringsten Privilegien und regelmäßigen Zugriffsüberprüfungen (Zugriff wird innerhalb von 24 Stunden nach Rollenwechsel oder Kündigung widerrufen)
- Single Sign-On (SSO) mit einem Identitätsanbieter
- Verschlüsselung von gespeicherten Daten auf Laptops/Notebooks
- Verschlüsselung mobiler Endgeräte
- Verschlüsselung von Wechseldatenträgern/mobilen Datenträgern
- Zuweisung eindeutiger Benutzerprofile zu IT-Systemen



Datenzugriffskontrolle

Maßnahmen, die sicherstellen, dass Personen, die zur Nutzung eines Datenverarbeitungssystems berechtigt sind, nur auf die personenbezogenen Daten zugreifen können, für die sie eine Berechtigung haben, und dass personenbezogene Daten während der Verarbeitung oder nach der Speicherung nicht ohne Berechtigung gelesen, kopiert, verändert oder entfernt werden können.

- Einrichtung eines Berechtigungs-/Autorisierungskonzepts
- Laufende Rechteverwaltung durch Systemadministratoren
- Sichere Aufbewahrung von Datenträgern
- Unternehmensweite Passwortstandards, einschließlich Mindestanforderungen an die Passwortlänge
- Restriktive Vergabe von Administratorrechten und erweiterte Admin-Schulungen, die über die allgemeine Mitarbeiterschulung hinausgehen
- Audit-Protokolle sind unveränderlich und zeitsynchronisiert (entsprechen einem Zeitplan, der auf gesetzliche, regulatorische und betriebliche Anforderungen abgestimmt ist)

Maßnahmen zur Gewährleistung der Trennung von Verarbeitungszwecken

Maßnahmen, die sicherstellen, dass Daten, die für unterschiedliche Zwecke erhoben werden, getrennt verarbeitet werden.

- Logische Mandantenfähigkeit (softwarebasiert)
- Definition und Durchsetzung von Regeln für den Datenbankzugriff

Maßnahmen zur Gewährleistung der Integrität (Art. 32 Abs. 1 Buchstabe b DSGVO)

Eingabekontrolle

Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder aus diesen gelöscht wurden.

- Führung einer Übersicht, aus der hervorgeht, mit welchen Anwendungen welche Daten eingegeben, geändert und gelöscht werden können

Übertragungskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten während der elektronischen Übertragung oder während des Transports oder der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mittels Datenübertragungseinrichtungen übermittelt werden dürfen.

- E-Mail-Verschlüsselung
- Transport Layer Security-Verschlüsselung für Daten während der Übertragung
- Verwendung von Standleitungen und/oder virtuellen privaten Netzwerktunneln



Maßnahmen zur Gewährleistung der Verfügbarkeit und Ausfallsicherheit (Art. 32 Abs. 1 Buchstabe b DSGVO)

Maßnahmen, die sicherstellen, dass personenbezogene Daten vor versehentlicher Zerstörung oder Verlust geschützt sind.

- Mehrere tägliche Datensicherungen, die in separaten Backup-Systemen gespeichert werden
- Backups werden verschlüsselt und in logisch getrennten EU/EWR-Konten oder -Regionen gespeichert (die Aufbewahrung erfolgt nach einem dokumentierten Zeitplan, der auf die Wiederherstellungsziele und gesetzlichen Anforderungen abgestimmt ist; Wiederherstellungstests finden regelmäßig statt)
- Kapazitätsmanagement mit Überwachung und automatischer Skalierung bei Kapazitätsengpässen
- Warnsystem zur Überwachung der Verfügbarkeit und des Server-/Systemstatus
- Das Wiederherstellungsziel beträgt maximal vierundzwanzig Stunden. Das Wiederherstellungsziel beträgt maximal vierundzwanzig Stunden für Produktionsdaten.
- IT-Incident-Management („Incident Response Management“) gemäß ISO/IEC 27002:2017 (einschließlich dokumentierter Verfahren für den Umgang mit Vorfällen und sicherheitsrelevanten Ereignissen)

Maßnahmen zur Gewährleistung einer effektiven Behandlung von Vorfällen:

- Matrix zur Klassifizierung und Eskalation von Vorfällen mit definierten Rollen
- Benachrichtigung der Kunden ohne unangemessene Verzögerung, nachdem eine meldepflichtige Verletzung des Schutzes personenbezogener Daten bekannt geworden ist
- Führung eines Verstoßprotokolls mit Fakten, Auswirkungen und Abhilfemaßnahmen
- Verfügbare Kontaktstelle in Vorfallsituationen
- Ursachenanalyse nach dem Vorfall und Plan für Korrekturmaßnahmen
- Bereitstellung eines zusammenfassenden Berichts nach dem Vorfall

Maßnahmen zur Gewährleistung regelmäßiger Tests, Bewertungen und Evaluierungen (Art. 32 Abs. 1 Buchstabe d DSGVO; Art. 25 Abs. 1 DSGVO)

Maßnahmen zur Beschreibung der Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen.

- Prozesse zur Analyse, Bewertung und Zuordnung von Risiken
- Prozesse zur Ableitung von Maßnahmen zur Risikominderung auf der Grundlage dieser Risiken
- Prozesse zur regelmäßigen Bewertung der Wirksamkeit dieser Maßnahmen

ANHANG 3: AUTORISIERTE UNTERAUFTRAGSVERARBEITER

Die folgenden Unternehmen sind autorisierte Unterauftragsverarbeiter im Sinne von Abschnitt „9.1 “ dieser DPA:



Dienstleistung (Anbieter)	Zweck	Adresse und Standort	Datenspeicherung	Sicherheit und Datenverarbeitung Dokumentationsdetails
Hetzner	Cloud-Infrastruktur (Verarbeitung und Speicherung)	Industriestr. 25 91710 Gunzenhausen Deutschland	Deutschland	https://www.hetzner.com/unternehmen/zertifizierung/
Render	Anwendungs-/Backend-Hosting, Datenbanken, Authentifizierung,	525 Brannan Street, Suite 300, San Francisco, CA 94107	Deutschland	https://render.com/docs/certifications-compliance
Google Cloud	Cloud-Infrastruktur (Google Cloud) und Produktivitäts-Tools (Google Workspace) zum Hosten, Verarbeiten und Unterstützen von Kundendaten.	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.	Deutschland	https://cloud.google.com/terms/data-processing-addendum
Microsoft	Cloud-Infrastruktur (Microsoft Azure) und Produktivitäts-Tools (Microsoft 365) zum Hosten, Verarbeiten und Unterstützen von Kundendaten.	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA	Deutschland	https://learn.microsoft.com/en-us/azure/compliance/offerings/
PostHog	Produktanalyse und Ereignistelemetrie.	2261 Market Street #4008, San Francisco, CA 94114	Deutschland	https://posthog.com/docs/privacy
Sentry	Fehleranalyse	45 Fremont Street, 8. Stock, San Francisco, CA 94105, USA	Deutschland	https://sentry.io/security/