

DATENSCHUTZ

Vertrag zur Auftragsverarbeitung

Nach Art. 28 DSGVO, auf Grundlage der Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/915). Die Klauseln sind unverändert übernommen; ausgefüllt sind die Anhänge I bis IV.

Gilt für: alle Leistungen, bei denen ich personenbezogene Daten in Ihrem Auftrag verarbeite

Stand: 18. Oktober 2026 · Version 1.0

So kommt der Vertrag zustande: Er ist Teil jedes Angebots, in dem ich personenbezogene Daten für Sie verarbeite. Mit der Annahme des Angebots stimmen Sie diesen Klauseln zu; die elektronische Form genügt (Art. 28 Abs. 9 DSGVO). Ihre Angaben in Anhang I trage ich im Angebot ein.

ABSCHNITT I

Klausel 1 Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll 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 (Datenschutz-Grundverordnung) sichergestellt werden.
- b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

- f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 Unabänderbarkeit der Klauseln

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 Auslegung

- a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 Kopplungsklausel (fakultativ)

Von den Parteien nicht vereinbart.

ABSCHNITT II

Pflichten der Parteien

Klausel 6 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 Anhang II aufgeführt.

Klausel 7 Pflichten der Parteien

7.1. Weisungen

- a) 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.
- b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

- a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III 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 (im Folgenden „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 gebührend Rechnung.
- b) 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.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogener 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 (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten 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 des Auftragsverarbeiters berücksichtigen.
- d) 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 durchgeführt.
- e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

- a) **Allgemeine schriftliche Genehmigung:** 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 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit 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.
- b) 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 diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- c) 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.
- d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang 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.
- e) 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.

7.8. Internationale Datenübermittlungen

- a) Jede 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 Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

- b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 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 Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 Unterstützung des Verantwortlichen

- a) 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.
- b) 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. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b 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:
- 1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 - 2) 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;
 - 3) 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;
 - 4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- d) Die Parteien legen in Anhang III 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.

Klausel 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle 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 Verordnung (EU) 2016/679 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.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

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

- a) 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);
- b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
 - 1) 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;
 - 2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - 3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls 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;

- c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, 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.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle 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:

- a) 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);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

- c) 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.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III

Schlussbestimmungen

Klausel 10 Verstöße gegen die Klauseln und Beendigung des Vertrags

- a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln 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.
- b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - 1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - 2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
 - 3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.
- c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln 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 gemäß Klausel 7.1 Buchstabe b verstoßen.
- d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I

Liste der Parteien

Verantwortlicher Kunde

Name

wird im Angebot eingetragen

Anschrift

wird im Angebot eingetragen

Kontaktperson (Name, Funktion, Kontaktdaten)

wird im Angebot eingetragen

Datenschutzbeauftragter

falls benannt: wird im Angebot eingetragen

Zustimmung und Datum

elektronisch mit Annahme des Angebots (Art. 28 Abs. 9 DSGVO)

Auftragsverarbeiter

Name

Maxim Lorkish, Einzelunternehmer, tätig unter „LORKISH“

Anschrift

Aue 82, 42103 Wuppertal, Deutschland

Kontaktperson (Name, Funktion, Kontaktdaten)

Maxim Lorkish, Inhaber · lorkish.commerce@gmail.com · +49 176 51481008

Datenschutzbeauftragter

nicht benannt; eine Pflicht zur Benennung besteht nicht (§ 38 Abs. 1 BDSG)

Zustimmung und Datum

elektronisch mit Übermittlung des Angebots

ANHANG II

Beschreibung der Verarbeitung

Die allgemeine Beschreibung gilt für jede Leistung, bei der ich im Auftrag des Verantwortlichen personenbezogene Daten verarbeite – auch für Leistungen, die unten nicht als Beispiel genannt sind. Die Einzelheiten stehen in der Leistungsbeschreibung des Angebots.

Allgemeine Beschreibung – gilt für jede Leistung

Gegenstand

Erbringung der im Angebot beschriebenen digitalen Leistungen, zum Beispiel Entwicklung, Betrieb und Betreuung von Websites, Chatbots, Apps, Automatisierungen und Schnittstellen sowie Wartung und Support. Was im Einzelfall verarbeitet wird, ergibt sich aus der Leistungsbeschreibung des Angebots; dort werden auch abweichende Fristen festgelegt.

Kategorien betroffener Personen

Kunden, Interessenten, Beschäftigte, Lieferanten und sonstige Geschäftspartner des Verantwortlichen sowie Nutzer seiner Websites, Anwendungen und Kommunikationskanäle – jeweils nur, soweit die beauftragte Leistung ihre Daten betrifft.

Kategorien personenbezogener Daten

Kontakt- und Stammdaten; Inhalte von Nachrichten, Anfragen, E-Mails und Dokumenten; Termin-, Vertrags-, Bestell- und Abrechnungsdaten; technische Nutzungs- und Verbindungsdaten (z. B. IP-Adresse, Zeitpunkte) – jeweils nur, soweit die beauftragte Leistung sie erfordert.

Art der Verarbeitung

Erheben, Speichern, Ordnen, Auslesen, Abgleichen und Übermitteln an die Systeme des Verantwortlichen; Erzeugen von Inhalten und Antworten mit KI-Sprachmodellen ausschließlich über Amazon Bedrock in der EU (Anhang IV); Sichern und Löschen; bei Wartung und Support auch der Zugriff auf Systeme und Daten des Verantwortlichen.

Zweck

Erbringung der im Angebot beschriebenen Leistung einschließlich Betrieb, Wartung, Fehlerbehebung und Support.

Dauer und Löschung

Für die Laufzeit des Hauptvertrags. Daten werden nur so lange gespeichert, wie die Leistung es erfordert: Zwischenspeicherungen spätestens nach 60 Tagen, Protokolle höchstens 28 Tage – soweit unten oder im Angebot keine andere Frist bestimmt ist.

Sensible Daten

Eine Verarbeitung sensibler Daten (Klausel 7.5) ist nicht vorgesehen; solche Daten werden nicht abgefragt. Gibt eine betroffene Person sie von sich aus ein, werden sie nur wie die übrigen Inhalte verarbeitet und mit ihnen gelöscht. Soll eine Leistung bewusst sensible Daten verarbeiten (z. B. Gesundheitsdaten), vereinbaren die Parteien vorher gesonderte Beschränkungen und Garantien.

Ort der Verarbeitung

Ausschließlich in Rechenzentren in der Europäischen Union (Server in Deutschland, KI-Sprachmodelle in AWS-Regionen der EU). Übermittlungen in Drittländer finden nicht statt.

Nach Vertragsende

Löschung oder Rückgabe nach Wahl des Verantwortlichen (Klausel 10 Buchstabe d) innerhalb von 60 Tagen, einschließlich aller Datensicherungen.

Unterauftragsverarbeiter

Gegenstand, Art und Dauer der Verarbeitung durch Unterauftragsverarbeiter: siehe Anhang IV. Braucht eine Leistung einen weiteren Unterauftragsverarbeiter, gilt Klausel 7.7 (Ankündigung mindestens 14 Tage im Voraus).

Besonderheiten typischer Leistungen

Für die folgenden Leistungen gelten ergänzend diese Angaben. Andere Leistungen beschreibt das Angebot nach demselben Muster.

A. KI-Chatbot für Website und WhatsApp

Kategorien betroffener Personen

Kunden, Interessenten und sonstige Personen, die dem Chatbot des Verantwortlichen auf dessen Website oder per WhatsApp schreiben; Beschäftigte des Verantwortlichen, die weitergeleitete Anfragen bearbeiten.

Kategorien personenbezogener Daten

Name und Kontaktdaten, soweit angegeben (Telefon- bzw. WhatsApp-Nummer, E-Mail-Adresse); Inhalte der Nachrichten; Termini (gewünschte Leistung, Datum, Uhrzeit); Zeitpunkt und Kanal der Nachricht; beim Website-Chat die für die Verbindung technisch nötigen Daten (z. B. IP-Adresse).

Art der Verarbeitung

Empfang und Speicherung der Nachrichten; Erzeugen von Antworten mit einem KI-Sprachmodell – dazu wird der jeweilige Gesprächsverlauf an Amazon Bedrock in Rechenzentren der EU übermittelt (Anhang IV); Eintragen von Terminen im Kalender des Verantwortlichen; Weiterleiten von Anfragen über die eigenen Kanäle des Verantwortlichen (sein E-Mail-Konto oder seine WhatsApp-Nummer); Löschung.

Zweck

Beantwortung von Anfragen der Kunden des Verantwortlichen, Vereinbarung von Terminen und Weiterleitung von Anliegen, die der Chatbot nicht abschließend beantworten kann.

Dauer und Löschung

Für die Laufzeit des Hauptvertrags. Gesprächsverläufe werden 180 Tage nach der letzten Nachricht automatisch gelöscht, sofern der Verantwortliche keine andere Frist bestimmt. Gebuchte Termine liegen im Kalendersystem des Verantwortlichen.

WhatsApp

Die WhatsApp-Business-Plattform nutzt der Verantwortliche im eigenen Namen auf Grundlage seiner Vereinbarungen mit Meta Platforms Ireland Ltd.; Meta ist kein Unterauftragsverarbeiter des Auftragsverarbeiters.

B. Website-Betreuung (Hosting und Wartung)

Kategorien betroffener Personen

Besucher der Website des Verantwortlichen; Personen, die über Formulare der Website Kontakt aufnehmen.

Kategorien personenbezogener Daten

Technische Zugriffsdaten (IP-Adresse, Datum und Uhrzeit, aufgerufene Adresse, Browserangaben); Inhalte von Formularen (z. B. Name, Kontaktdaten, Nachricht).

Art der Verarbeitung

Speichern und Ausliefern der Website (Hosting); Weiterleiten von Formularanfragen an den Verantwortlichen über dessen eigenes E-Mail-Konto; Wartung, Datensicherung und Löschung.

Zweck

Bereitstellung, sicherer Betrieb und Wartung der Website; Weiterleitung von Anfragen.

Dauer und Löschung

Für die Laufzeit des Hauptvertrags. Zugriffsprotokolle höchstens 28 Tage; Formularinhalte nach erfolgreicher Weiterleitung höchstens 60 Tage, um Zustellprobleme nachverfolgen zu können.

C. KI-Automatisierung von Abläufen

Kategorien betroffener Personen

Kunden, Interessenten, Lieferanten und Beschäftigte des Verantwortlichen, soweit ihre Daten in den automatisierten Abläufen vorkommen.

Kategorien personenbezogener Daten

Kontakt- und Stammdaten; Anfrage- und Termindaten; Inhalte von E-Mails und Anhängen, soweit sie den Ablauf betreffen; Rechnungsdaten (z. B. Rechnungsnummer, Beträge, Bankverbindung auf Eingangsrechnungen).

Art der Verarbeitung

Abruf aus und Übergabe an die Systeme des Verantwortlichen (z. B. E-Mail-Postfach, CRM, Kalender, Buchhaltungssoftware) über deren Schnittstellen; Auslesen und Zuordnen von Inhalten, auch mit einem KI-Sprachmodell über Amazon Bedrock in Rechenzentren der EU; kurzzeitige Zwischenspeicherung; Ablaufprotokolle; Löschung.

Zweck

Durchführung der im Angebot beschriebenen Abläufe.

Dauer und Löschung

Für die Laufzeit des Hauptvertrags. Zwischenspeicherungen werden nach Abschluss des jeweiligen Ablaufs gelöscht, spätestens nach 60 Tagen; Ablaufprotokolle höchstens 60 Tage. Im Übrigen verbleiben die Daten in den Systemen des Verantwortlichen.

ANHANG III

Technische und organisatorische Maßnahmen

Diese Maßnahmen gelten für alle Leistungen aus Anhang II und werden mindestens jährlich überprüft.

1. Verschlüsselung bei Übertragung und Speicherung

- Alle Verbindungen zu Websites, Chat und Schnittstellen laufen ausschließlich über HTTPS (TLS); die Zertifikate werden automatisch erneuert.
- Verbindungen zu Amazon Bedrock und zu den Systemen des Verantwortlichen sind stets verschlüsselt (TLS).
- Datensicherungen werden vor dem Verlassen des Servers mit AES-256 verschlüsselt.
- Der Arbeitsrechner des Auftragsverarbeiters ist vollständig verschlüsselt (Geräteverschlüsselung).

2. Identifizierung, Zugang und Berechtigungen

- Zugriff auf Server und Daten hat ausschließlich der Auftragsverarbeiter persönlich; es gibt keine weiteren Beschäftigten. Er ist zur Vertraulichkeit verpflichtet.
- Zugang zu den Servern nur mit SSH-Schlüssel; die Anmeldung per Passwort ist abgeschaltet.
- Die Verwaltungskonten für Hosting und Cloud-Dienste sind mit Zwei-Faktor-Authentifizierung geschützt.
- Wiederholte fehlgeschlagene Anmeldeversuche werden automatisch gesperrt.

3. Systemkonfiguration und Trennung der Daten

- Firewall: Aus dem Internet erreichbar sind nur die Ports für Web (80, 443) und SSH (22); Datenbanken und interne Dienste sind nicht öffentlich erreichbar.
- Jede Anwendung läuft in einem eigenen Container ohne Administratorrechte; die Daten verschiedener Verantwortlicher werden getrennt gespeichert.
- Sicherheitsupdates des Betriebssystems werden automatisch eingespielt; Anwendungen werden regelmäßig aktualisiert.
- Änderungen an Anwendungen werden vor dem Einsatz mit automatischen Tests geprüft.

4. Physische Sicherheit

- Die Server stehen in Rechenzentren der Hetzner Online GmbH in Deutschland; Rechenzentren und Hosting-Dienste sind nach ISO/IEC 27001:2022 zertifiziert.

5. Verfügbarkeit und rasche Wiederherstellung

- Die Daten des Verantwortlichen werden täglich verschlüsselt gesichert; die letzten 7 Sicherungen liegen auf dem Server, eine zusätzliche Kopie wird auf den verschlüsselten Arbeitsrechner des Auftragsverarbeiters übertragen.
- Die Wiederherstellung wird vor der Inbetriebnahme und danach mindestens halbjährlich getestet.
- Anwendungen starten nach Störungen automatisch neu.

6. Protokollierung

- Administrative Anmeldungen am Server werden im Systemprotokoll erfasst.
- Anwendungsprotokolle enthalten keine Nachrichteninhalte und werden höchstens 28 Tage aufbewahrt.

7. Datenminimierung, begrenzte Speicherung, Löschung und Übertragbarkeit

- Verarbeitet werden nur Daten, die für den jeweiligen Zweck nötig sind; das KI-Sprachmodell erhält nur den jeweiligen Gesprächsverlauf bzw. die zu verarbeitenden Inhalte.
- Automatische Löschung nach den Fristen in Anhang II.
- Die Daten des Verantwortlichen werden nicht zum Training von KI-Modellen verwendet; bei Amazon Bedrock ist die Protokollierung der Modellaufrufe abgeschaltet, Eingaben werden nicht über die Anfrage hinaus gespeichert.
- Die KI-Sprachmodelle werden über das geografische Profil „EU“ mit der Quellregion Frankfurt (eu-central-1) angesprochen; Anfragen werden dabei nur an AWS-Regionen innerhalb der EU geleitet.
- In Entwicklung und Test werden keine echten personenbezogenen Daten verwendet, sondern Testdaten oder anonymisierte Daten.
- Auf Weisung werden Gesprächsverläufe und weitere Daten in einem gängigen Format (z. B. CSV oder JSON) herausgegeben oder einzeln gelöscht.

8. Transparenz beim Einsatz von KI

- Der Chatbot gibt sich zu Beginn des Gesprächs als KI zu erkennen (Art. 50 Verordnung (EU) 2024/1689).
- Der Chatbot trifft keine Entscheidungen mit rechtlicher Wirkung im Sinne von Art. 22 DSGVO; Anliegen außerhalb seines Wissens gibt er an den Verantwortlichen weiter.

9. Rechenschaft und Überprüfung

- Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
- Diese Maßnahmen werden mindestens jährlich sowie bei wesentlichen Änderungen überprüft; Änderungen werden dokumentiert.

10. Unterstützung des Verantwortlichen (Klauseln 8 und 9)

- Anfragen betroffener Personen, die beim Auftragsverarbeiter eingehen, leitet er innerhalb von 6 Werktagen an den Verantwortlichen weiter.
- Auskunft, Berichtigung, Löschung oder Export einzelner Datensätze setzt er auf Weisung unverzüglich um, in der Regel innerhalb von 10 Werktagen.
- Verletzungen des Schutzes personenbezogener Daten meldet er unverzüglich, spätestens 48 Stunden nachdem sie ihm bekannt wurden, per E-Mail und telefonisch.
- Auf Anfrage stellt er die Informationen bereit, die der Verantwortliche für eine Datenschutz-Folgenabschätzung benötigt.

ANHANG IV

Liste der Unterauftragsverarbeiter

Der Verantwortliche genehmigt die Inanspruchnahme der folgenden Unterauftragsverarbeiter (allgemeine schriftliche Genehmigung, Klausel 7.7 Buchstabe a). Änderungen dieser Liste kündigt der Auftragsverarbeiter mindestens 14 Tage im Voraus an.

1. Hetzner Online GmbH

Anschrift

Industriestr. 25, 91710 Gunzenhausen, Deutschland

Kontaktperson

Datenschutzbeauftragter der Hetzner Online GmbH · data-protection@hetzner.com · +49 9831 505-216

Beschreibung der Verarbeitung

Bereitstellung der Server, auf denen alle Leistungen betrieben und alle Daten gespeichert werden (Rechenzentrum Nürnberg, Deutschland). Gilt für alle Leistungen.

Garantien

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO; Verarbeitung ausschließlich in der EU; Zertifizierung nach ISO/IEC 27001:2022 und Testat nach BSI C5 Typ 2.

2. Amazon Web Services EMEA SARL

Anschrift

38 Avenue John F. Kennedy, L-1855 Luxemburg

Kontaktperson

Data Protection, Anschrift wie oben

Beschreibung der Verarbeitung

Bereitstellung von KI-Sprachmodellen über den Dienst Amazon Bedrock: Gesprächsverläufe bzw. zu verarbeitende Inhalte werden verarbeitet, um Antworten zu erzeugen. Verarbeitung ausschließlich in AWS-Regionen der EU, keine Speicherung über die Anfrage hinaus, keine Nutzung zum Training. Gilt für alle Leistungen, die KI-Sprachmodelle nutzen.

Garantien

AWS-Datenverarbeitungsnachtrag (AWS GDPR Data Processing Addendum) einschließlich der Standardvertragsklauseln der Europäischen Kommission.

Quelle der Klauseln: Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, ABl. L 199 vom 7.6.2021, S. 18. · Stand: 18. Oktober 2026 · Version 1.0