Vertrag über die Auftragsverarbeitung personenbezogener Daten

Version 1.2, Stand: 2026 | Dialogine GmbH | c/o Gateway Workspace Weyertal 109 50931 Köln | www.hi-desk.de | Handelsregister Amtsgericht Köln HRB 125527
USt-IdNr: DE459155272 | Bankverbindung DE46 3707 0209 0077 7458 00

1. Standardvertragsklauseln

Die Parteien stimmen dem Text des Durchführungsbeschlusses (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 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates zu.

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

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

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 personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche

Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (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 Kalendertage 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

Verantwortlicher

Die vom Kunden im HiDesk-Konto benannte Administrator-Person gilt als primäre Ansprechperson und Empfängerin sämtlicher Mitteilungen im Zusammenhang mit diesem Vertrag. Bis zur Benennung dieser Person werden Mitteilungen an die Person gerichtet, die spätestens zu Beginn der Nutzung der HiDesk-Plattform als Administrator im Kundenkonto hinterlegt ist.

Auftragsverarbeiter
c/o Gateway Workspace
Dialogine GmbH
Weyertal 109
50931 Köln

Datenschutzkontakt:

privacy@hi-desk.de

Anhang II – Beschreibung der Verarbeitung

1. Gegenstand

Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der HiDesk-Plattform, die von der Dialogine GmbH betrieben wird. Die Plattform ermöglicht den Betrieb digitaler Telefonassistenten zur automatisierten Gesprächsannahme, Weiterleitung, Protokollierung und Bearbeitung von Telefonanrufen. Die Dialogine GmbH verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung der Kundschaft. Die Verantwortung für die Rechtmäßigkeit der Datenerhebung und -übermittlung liegt bei der Kundschaft.

2. Dauer

Die Verarbeitung erfolgt für die Dauer des zwischen der Kundschaft und der Dialogine GmbH bestehenden Vertragsverhältnisses über die Nutzung der HiDesk-Plattform. Nach Beendigung des Vertrags werden personenbezogene Daten – sofern keine gesetzlichen Aufbewahrungspflichten bestehen – gemäß den Bestimmungen dieses Auftragsverarbeitungsvertrags gelöscht oder auf Wunsch an die Kundschaft zurückgegeben.

3. Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zur Erbringung der vereinbarten Leistungen im Rahmen der HiDesk-Plattform, insbesondere zur:

- automatisierten Entgegennahme und Beantwortung von Telefonanrufen,
- Weiterleitung von Anrufen oder Nachrichten,
- Terminvereinbarung und -bestätigung,
- Erstellung und Bereitstellung von Gesprächsprotokollen und Transkripten,
- System- und Nutzungsanalyse zur Qualitätssicherung,
- Abrechnung und technischen Administration der Dienstleistung.

4. Art der personenbezogenen Daten

Im Rahmen der Leistungserbringung können insbesondere folgende personenbezogene Daten verarbeitet werden:

- Stammdaten (z. B. Name, Telefonnummer, ggf. E-Mail-Adresse),
- Gesprächsinhalte und Transkripte,
- Termin- und Kommunikationsdaten (Datum, Uhrzeit, Dauer, Gesprächspartner),
- technische Metadaten (z. B. IP-Adressen, Verbindungsinformationen, Logdaten),
- Zahlungs- und Abrechnungsdaten, soweit erforderlich,
- Gesprächsinhalte und Transkripte, die sensible Daten gem. Art. 9 Abs. 1 DSGVO enthalten können (insbesondere Gesundheitsdaten wie Symptome, Diagnosen, Behandlungswünsche oder Terminanlässe, die Rückschlüsse auf den Gesundheitszustand der anrufenden Person zulassen).

5. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind insbesondere:

- **Anrufende Personen**, also Kundschaft, Interessierte, Patienten oder Geschäftspartner des Kunden,
- **Mitarbeitende des Kunden**, die mit der Nutzung, Verwaltung oder Auswertung der HiDesk-Plattform befasst sind,
- ggf. weitere vom Kunden benannte Kontaktpersonen.

Anhang III – Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Die Dialogine GmbH trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Die Maßnahmen berücksichtigen den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung. Sie werden regelmäßig überprüft und bei Bedarf angepasst, um den Schutz personenbezogener Daten sicherzustellen. Alle Mitarbeiter des Auftragsverarbeiters, die Zugriff auf Patientendaten (Art. 9 DSGVO) haben können, sind schriftlich zur Vertraulichkeit verpflichtet und über die besondere Relevanz der ärztlichen Schweigepflicht belehrt.

1. Zutrittskontrolle (physische Sicherheit)

- Betrieb sämtlicher Systeme in gesicherten Rechenzentren des Hosting-Partners (Netcup, Nürnberg).
- Zutritt zu Büroräumen nur für berechtigte Personen.
- Keine physische Speicherung personenbezogener Daten auf Papier.

2. Zugangskontrolle (digitale Zugangssicherung)

- Zugriff auf Systeme nur über individuelle Benutzerkonten mit starken Passwörtern.
- Zwei-Faktor-Authentifizierung (2FA) für administrative Zugänge.
- Regelmäßige Überprüfung und Deaktivierung inaktiver Konten.

3. Zugriffskontrolle (Rechtevergabe innerhalb der Systeme)

- Rollenbasiertes Berechtigungskonzept mit minimalen Zugriffsrechten („Need-to-know"-Prinzip).
- Zugriff auf personenbezogene Daten nur durch autorisierte Personen.
- Protokollierung und Nachvollziehbarkeit administrativer Zugriffe.

4. Weitergabekontrolle

- Datenübertragung ausschließlich über verschlüsselte Verbindungen.
- Keine unverschlüsselte Weitergabe sensibler Informationen.
- Subdienstleister werden ausschließlich auf Grundlage eines Auftragsverarbeitungsvertrags eingebunden.

5. Eingabekontrolle

- Protokollierung von Änderungen und Administrativen Zugriffen.

- Nachvollziehbarkeit der Datenverarbeitung durch interne Logging-Systeme.

6. Auftragskontrolle

- Schriftliche Vereinbarungen mit allen Sub-Auftragsverarbeitern (vgl. Anhang IV).
- Prüfung der von Subdienstleistern veröffentlichten Sicherheitsnachweise (z.B. ISO 27001, SOC 2).

7. Maßnahmen zum Schutz der Daten währen der Speicherung

Personenbezogene Daten werden auf Systemen gespeichert, die nach dem Stand der Technik gegen unbefugten Zugriff und Verlust geschützt sind. Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Integrität und Verfügbarkeit der gespeicherten Daten. Dazu können – je nach Risiko und technischer Umsetzbarkeit – Verschlüsselungs-, Backup- und Zugriffsbeschränkungsmechanismen gehören. Die konkreten Verfahren und Intervalle werden nach Maßgabe des Stands der Technik, der Implementierungskosten und des jeweiligen Risikos festgelegt und regelmäßig überprüft.

8. Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

- Rechenzentren mit Zugangsbeschränkung, Videoüberwachung und 24/7-Sicherheitsdienst.
- Zutritt zu Unternehmensräumen nur für autorisierte Personen.

9. Maßnahmen zu Sicherstellung von Protokollierung, Systemkonfiguration, Governance und Qualität.

- Protokollierung: Administrativer Zugriff und sicherheitsrelevante Ereignisse werden protokolliert, um Änderungen und Zugriffe nachvollziehbar zu machen.
- Systemkonfiguration: Systeme werden nach anerkannten Sicherheitsstandards konfiguriert („Security by Default“) und regelmäßig aktualisiert.
- Interne IT-Governance: Zuständigkeiten für Datenschutz und IT-Sicherheit sind festgelegt; sicherheitsrelevante Entscheidungen werden dokumentiert.
- Qualitätssicherung: Dienstleister mit geeigneten Zertifizierungen (z. B. ISO 27001, SOC 2) bevorzugt.

10. Maßnahmen zur Datenminimierung, Datenqualität und Speicherbegrenzung

- Es werden nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet („Need-to-know“-Prinzip).
- Nicht mehr benötigte oder fehlerhafte Daten werden berichtigt, anonymisiert oder gelöscht.
- Automatisierte Löschprozesse und feste Speicherfristen (z. B. regelmäßige Löschung von Gesprächsdaten und Protokollen) gewährleisten eine begrenzte Datenspeicherung.

11. Maßnahmen zur Rechenschaftspflicht, Übertragbarkeit und Löschung

- Datenschutzmaßnahmen werden dokumentiert und regelmäßig überprüft.
- Auf Anfrage des Kunden kann Dialogine personenbezogene Daten in einem gängigen, maschinenlesbaren Format bereitstellen.
- Nach Vertragsende erfolgt eine vollständige Löschung oder Rückgabe der personenbezogenen Daten; der Löschvorgang wird protokolliert.

12. Maßnahmen bei Datenübermittlungen an Unterauftragsverarbeiter

- Auswahl ausschließlich DSGVO-konformer Subdienstleister.
- Abschluss schriftlicher Auftragsverarbeitungsverträge mit gleichwertigen Sicherheitsstandards.

- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen der Sub-Auftragsverarbeiter.

Anhang IV – Liste der Unterauftragsverarbeiter

Die Dialogine GmbH setzt zur Bereitstellung und zum Betrieb der HiDesk-Plattform ausgewählte Unterauftragsverarbeiter ein, die im Auftrag von Dialogine personenbezogene Daten der Kundschaft verarbeiten. Diese Unterauftragsverarbeiter sind durch vertragliche Vereinbarungen an die in diesem Auftragsverarbeitungsvertrag festgelegten Datenschutz- und Sicherheitsanforderungen gebunden.

Um die Einhaltung der Bestimmungen zu gewährleisten, führt Dialogine regelmäßige Überprüfungen seiner Unterauftragsverarbeiter durch und verlangt von ihnen, geeignete technische und organisatorische Maßnahmen zu ergreifen. Diese Maßnahmen sollen die Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen gewährleisten.

In der nachstehenden Liste sind die derzeit eingesetzten Unterauftragsverarbeiter aufgeführt, die zur Erbringung und Aufrechterhaltung der HiDesk-Dienstleistungen eingesetzt werden.

Anbieter	*Zweck der Verarbeitung*	*Sitz / Hosting-Ort*	*URL*
Assembly	STT Modelle (Opt-In)	US/EU	https://www.assemblyai.com/
AWS	Nutzung von Realtime und LLM Modellen (Opt-In)	USA / EU (Schweden)	https://aws.amazon.com/
Cerebras	Schnelle LLM Inferenz (Opt-In)	US/US	https://www.cerebras.ai/
Cloudflare	Bot Schutz	US/Global	https://www.cloudflare.com/
Dashscope	LLM Inferenz (Qwen Modelle)	CN/EU	https://www.alibabacloud.com/
Deepslate	Realtime Modelle (Opt-In)	EU/EU	https://deepslate.eu/
Firecrawl	Web-Scraping und Datenanreicherung	USA / EU (je nach Einsatzregion)	www.firecrawl.dev
Google Cloud	Nutzung von LLM-, Voice-to-Voice- und TTS-Modellen (Opt-In)	USA / EU (Niederlande)	www.cloud.google.com
Hetzner	Hosting, Object-Storage und Datenbankbetrieb	DE/DE (Nürnberg)	https://www.hetzner.com/
Infisical	Customer Secret Management	US/EU	https://eu.infisical.com
KugelAudio	TTS Modelle (Opt-In)	EU/EU	https://kugelaudio.com/de

Anbieter	*Zweck der Verarbeitung*	*Sitz / Hosting-Ort*	*URL*
Microsoft Azure	Nutzung von Voice-to-Voice- und TTS-Modellen (Opt-In)	USA / EU (Schweden)	www.portal.azure.com
Mistral	STT, TTS, LLM Inferenz (Opt-In)	EU/EU	https://mistral.ai/
PostHog	Produkt- und Nutzungsanalyse (EU-Cluster)	USA / EU	www.eu.posthog.com
Lettermint B.V.	E-Mail-Versand und Zustellung (Transactional Email)	EU / Niederlande	https://lettermint.com
Stripe	Abrechnung und Verbrauchsmessung	US / US (Data Privacy Framework)	www.stripe.com/en-de
Telnyx	Telefonie-Provider (Sprachübertragung, Aufnahme und Rufweiterleitung)	USA / EU (Region Deutschland)	https://telnyx.com/
Twilio	Telefonie-Provider (Sprachübertragung, Aufnahme und Rufweiterleitung)	USA / EU (Irland)	https://www.twilio.com/de-de
Vonage	Telefonie-Provider (Sprachübertragung, Aufnahme und Rufweiterleitung)	US / EU	www.vonage.com

Optionale Integrationspartner

Die folgenden Sub-Unternehmer werden ausschließlich verarbeitet, wenn der Kunde die jeweilige Integration aktiviert. Ohne Aktivierung findet keine Datenübermittlung statt. Der Hosting Ort ist abhängig davon, wo der Endkunde sein Hosting hat und kann nicht pauschal festgestellt werden.

Anbieter	*Zweck der Verarbeitung*	*Sitz / Hosting-Ort*	*URL*
anny	Buchungen	EU/EU	https://anny.co/
Cal.com	Kalender-Integration	US/EU	https://cal.com
Hubspot	Optionale Integration, CRM	US/EU	https://hubspot.com
Meetergo	Optionale Integration, Termine	EU/EU	https://meetergo.com/
Shopify	Optionale Integration, E-Commerce	US/US	https://www.shopify.com/de