Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Version: Oktober 2026

PRÄAMBEL

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Auftragsverhältnis im Sinne des Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), EU-DSGVO.
Dem Verantwortlichen und dem Auftragsverarbeiter ist bekannt, dass sich die Vorgaben zur Auftragsverarbeitung nach der DSGVO in ihrer jeweils gültigen Form richten.
Der Verantwortliche und der Auftragsverarbeiter vereinbaren die nachfolgenden Standardvertragsklauseln zur Erfüllung der Anforderungen gemäß Art. 28 EU-DSGVO, um angemessene Garantien (in Bezug auf den Schutz der Privatsphäre und der Grundrechte und -freiheiten natürlicher Personen) für die in Anhang II der Klauseln beschriebenen Verarbeitung zu schaffen.

STANDARDVERTRAGSKLAUSELN

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 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

Nicht genutzt.

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 30 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

Verantwortlicher im Sinne des Datenschutzes und Kontaktperson ist der Auftraggeber.

Auftragsverarbeiter

Auftragsverarbeiter		Datenschutzbeauftragter*		Kontaktperson		
Name	Anschrift	Name	Kontaktdaten	Name	Funktion	Kontaktdaten
cloudworx GmbH	Rupert-Mayer-Straße 44, 81379 München	Timo Müller	Rupert-Mayer-Straße 44, 81379 München E-Mail: privacy@cloudworx.agency	Timo Müller	Geschäftsführer	Rupert-Mayer-Straße 44, 81379 München Tel.: +49 800 25 68 396 E-Mail: info@cloudworx.agency

* **Hinweis:** Cloudworx ist nicht verpflichtet einen Datenschutzbeauftragten zu bestellen. Bei Fragen zum Datenschutz steht die Geschäftsleitung als Ansprechpartner zur Verfügung.

ANHANG II – Beschreibung der Verarbeitung

Hinweis: Die nachfolgend beschriebenen Verarbeitungen werden von Cloudworx als SaaS-Lösung angeboten. Die tatsächliche Verarbeitung richtet sich nach dem Hauptvertrag.

in.bounz in.bounz ist eine Lösung für die Überwachung von E-Mail Postfächern sowie die automatisierte und kontextbezogene Dokumentation in Salesforce.
Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
Kunden Mitarbeiter Lieferanten Endnutzer
Kategorien personenbezogener Daten, die verarbeitet werden
Stammdaten und Kommunikationsdaten der Cloudworx-Konten von Kunden. IT-System-spezifische Daten, wie z.B. User-Name, Zugriffsrechte, IP-Adressen. Kundendaten, die unter den E-Mail Konten des Kunden durch den Service verarbeitet werden.
Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangs-beschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
Sensible Kundendaten, die unter den E-Mail Konten des Kunden durch den Service verarbeitet werden. Angewandte Beschränkungen und Garantien: Strenge Zweckbindung, Zugangsbeschränkungen, Zugang nur für Cloudworx-Mitarbeiter, die eine spezielle Schulung absolviert haben, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen.
Art der Verarbeitung
Berechnung, Verarbeitung, Speicherung, Synchronisation und andere Dienste, wie in der Dokumentation beschrieben und vom Kunden von Zeit zu Zeit veranlasst.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Dokumentation von E-Mails. Synchronisation mit Salesforce. Fernwartung, Service und Support.
Dauer der Verarbeitung
Entsprechend der Laufzeit des Hauptvertrages.
Verarbeitung durch (Unter-)Auftragsverarbeiter. Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter

sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Subunternehmer 1: Host Europe GmbH Gegenstand: Speicherung und Backup von Kundendaten. Art: Verarbeitung, Speicherung und Übermittlung von Daten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 2: Scalyr, LLC (vormals Scalyr, Inc.; DataSet, Unternehmen der SentinelOne-Gruppe) Gegenstand: SaaS-Plattform für das Protokoll-Management und die Server-Überwachung. Art: Verarbeitung, Speicherung und Übermittlung von Protokolldaten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.

out.bounz out.bounz ist eine Lösung für den manuellen, teilautomatischen und vollautomatischen Versand von E-Mails aus Salesforce.
Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
Kunden Mitarbeiter Lieferanten Endnutzer
Kategorien personenbezogener Daten, die verarbeitet werden
Stammdaten und Kommunikationsdaten der Cloudworx-Konten von Kunden. IT-System-spezifische Daten, wie z.B. User-Name, Zugriffsrechte, IP-Adressen. Kundendaten, die unter den E-Mail Konten des Kunden durch den Service verarbeitet werden.
Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangs-beschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
Sensible Kundendaten, die unter den E-Mail Konten des Kunden durch den Service verarbeitet werden. Angewandte Beschränkungen und Garantien: Strenge Zweckbindung, Zugangsbeschränkungen, Zugang nur für Cloudworx-Mitarbeiter, die eine spezielle Schulung absolviert haben, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen.
Art der Verarbeitung
Berechnung, Verarbeitung, Speicherung, Synchronisation und andere Dienste, wie in der Dokumentation beschrieben und vom Kunden von Zeit zu Zeit veranlasst.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Versand und Dokumentation von E-Mails. Synchronisation mit Salesforce. Fernwartung, Service und Support.
Dauer der Verarbeitung
Entsprechend der Laufzeit des Hauptvertrages.
Verarbeitung durch (Unter-)Auftragsverarbeiter. Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Subunternehmer 1: Host Europe GmbH Gegenstand: Speicherung und Backup von Kundendaten. Art: Verarbeitung, Speicherung und Übermittlung von Daten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 2: Scalyr, LLC (vormals Scalyr, Inc.; DataSet, Unternehmen der SentinelOne-Gruppe) Gegenstand: SaaS-Plattform für das Protokoll-Management und die Server-Überwachung. Art: Verarbeitung, Speicherung und Übermittlung von Protokolldaten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.

millio
millio ist eine Banking-Lösung für Salesforce. Transaktionsdaten können automatisiert in Salesforce gespeichert und Zahlungen und Lastschriften ausgeführt werden.
Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
Kunden Mitarbeiter Lieferanten Endnutzer
Kategorien personenbezogener Daten, die verarbeitet werden
Stammdaten und Kommunikationsdaten der Cloudworx-Konten von Kunden. IT-System-spezifische Daten, wie z.B. User-Name, Zugriffsrechte, IP-Adressen. Bank- und Transaktionsdaten, z. B. Kontoinhaber, IBAN, Umsätze und Verwendungszwecke.

Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
Sensible Kundendaten aus dem Salesforce-System des Kunden. Angewandte Beschränkungen und Garantien: Strenge Zweckbindung, Zugangsbeschränkungen, Zugang nur für Cloudworx-Mitarbeiter, die eine spezielle Schulung absolviert haben, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen, Verschlüsselung.
Art der Verarbeitung
Berechnung, Verarbeitung, Speicherung, Synchronisation und andere Dienste, wie in der Dokumentation beschrieben.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Abruf von Kontoumsätzen sowie Ausführung von Zahlungen und Lastschriften über die angebundene Bankschnittstelle. Synchronisation mit Salesforce. Fernwartung, Service und Support.
Dauer der Verarbeitung
Entsprechend der Laufzeit des Hauptvertrages.
Verarbeitung durch (Unter-)Auftragsverarbeiter. Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Subunternehmer 1: Host Europe GmbH Gegenstand: Speicherung und Backup von Kundendaten. Art: Verarbeitung, Speicherung und Übermittlung von Daten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 2: Scalyr, LLC (vormals Scalyr, Inc.; DataSet, Unternehmen der SentinelOne-Gruppe) Gegenstand: SaaS-Plattform für das Protokoll-Management und die Server-Überwachung. Art: Verarbeitung, Speicherung und Übermittlung von Protokolldaten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 3: finAPI GmbH Gegenstand: Schnittstelle zum Abrufen von Bankdaten und Übertragen von Daten an Banken. Art: Verarbeitung, Speicherung und Übermittlung von Bankdaten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.

REEDR REEDR ist ein KI-basierter OCR-Assistent für automatisierte Texterkennung und die intelligente Extraktion strukturierter Daten aus jeglichen Dokumenten – beispielsweise Rechnungen, Ausweisdokumenten, Fahrzeugscheinen und vielen weiteren. REEDR kann entweder auf Basis von KI oder anhand festgelegter Regeln agieren.
Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
Kunden Mitarbeiter Lieferanten Endnutzer
Kategorien personenbezogener Daten, die verarbeitet werden
Stammdaten und Kommunikationsdaten der Cloudworx-Konten von Kunden. IT-System-spezifische Daten, wie z.B. User-Name, Zugriffsrechte, IP-Adressen. Inhalte der zur Verarbeitung übermittelten Dokumente, z. B. Rechnungen, Ausweisdokumente und Fahrzeugscheine.
Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangs-beschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
Sensible Kundendaten aus dem Salesforce-System des Kunden. Angewandte Beschränkungen und Garantien: Strenge Zweckbindung, Zugangsbeschränkungen, Zugang nur für Cloudworx-Mitarbeiter, die eine spezielle Schulung absolviert haben, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen, Verschlüsselung.
Art der Verarbeitung
Berechnung, Verarbeitung, Speicherung, Synchronisation und andere Dienste, wie in der Dokumentation beschrieben.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Auslesen und Extraktion strukturierter Daten aus Dokumenten. Synchronisation mit Salesforce. Fernwartung, Service und Support.
Dauer der Verarbeitung
Entsprechend der Laufzeit des Hauptvertrages.
Verarbeitung durch (Unter-)Auftragsverarbeiter. Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Subunternehmer 1: Host Europe GmbH Gegenstand: Speicherung und Backup von Kundendaten. Art: Verarbeitung, Speicherung und Übermittlung von Daten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 2: Scalyr, LLC (vormals Scalyr, Inc.; DataSet, Unternehmen der SentinelOne-Gruppe) Gegenstand: SaaS-Plattform für das Protokoll-Management und die Server-Überwachung. Art: Verarbeitung, Speicherung und Übermittlung von Protokolldaten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 3: Doxis AI Solutions B.V. (vormals Klippa App B.V.) Gegenstand: Schnittstelle zum Übertragen der vom Endkunden übermittelten Dokumente zum Auslesen und Verarbeiten mit Hilfe von künstlicher Intelligenz (KI). Art: Verarbeitung, Speicherung und Übermittlung von Dokumenten des Endkunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 4: Hypatos GmbH Gegenstand: Schnittstelle zum Übertragen der vom Endkunden übermittelten Dokumente zum Auslesen und Verarbeiten mit Hilfe von künstlicher Intelligenz (KI). Art: Verarbeitung, Speicherung und Übermittlung von Dokumenten des Endkunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 5: Natif.ai GmbH Gegenstand: Schnittstelle zum Übertragen der vom Endkunden übermittelten Dokumente zum Auslesen und Verarbeiten mit Hilfe von künstlicher Intelligenz (KI). Art: Verarbeitung, Speicherung und Übermittlung von Dokumenten des Endkunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.

integraid integraid ist eine Anwendung, die sichere und schnelle API-Integrationen in Salesforce ermöglicht. Dabei werden Daten aus verschiedenen Apps, Plattformen und Systemen über standardisierte Schnittstellen eingebunden. Dies erleichtert die automatisierte Übertragung relevanter Informationen und den reibungslosen Datenaustausch innerhalb eines Unternehmens.
Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
Kunden Mitarbeiter

Lieferanten Endnutzer
Kategorien personenbezogener Daten, die verarbeitet werden
Stammdaten und Kommunikationsdaten der Cloudworx-Konten von Kunden. IT-System-spezifische Daten, wie z.B. User-Name, Zugriffsrechte, IP-Adressen. Kundendaten, die über die konfigurierten Schnittstellen zwischen Salesforce und Drittsystemen übertragen werden.
Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangs-beschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
Sensible Kundendaten, die über die konfigurierten Schnittstellen zwischen Salesforce und Drittsystemen übertragen werden. Angewandte Beschränkungen und Garantien: Strenge Zweckbindung, Zugangsbeschränkungen, Zugang nur für Cloudworx-Mitarbeiter, die eine spezielle Schulung absolviert haben, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen.
Art der Verarbeitung
Berechnung, Verarbeitung, Speicherung, Synchronisation und andere Dienste, wie in der Dokumentation beschrieben und vom Kunden von Zeit zu Zeit veranlasst.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Datenaustausch zwischen Salesforce und Drittsystemen über Schnittstellen. Synchronisation mit Salesforce. Fernwartung, Service und Support.
Dauer der Verarbeitung
Entsprechend der Laufzeit des Hauptvertrages.
Verarbeitung durch (Unter-)Auftragsverarbeiter. Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Subunternehmer 1: Host Europe GmbH Gegenstand: Speicherung und Backup von Kundendaten. Art: Verarbeitung, Speicherung und Übermittlung von Daten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 2: Scalyr, LLC (vormals Scalyr, Inc.; DataSet, Unternehmen der SentinelOne-Gruppe) Gegenstand: SaaS-Plattform für das Protokoll-Management und die Server-Überwachung. Art: Verarbeitung, Speicherung und Übermittlung von Protokolldaten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und

Supportvereinbarung.

XRSF XRSF ist eine Anwendung zur Verarbeitung elektronischer Rechnungen direkt in Salesforce. Das Tool ermöglicht die Erstellung und das Auslesen von Rechnungen in verschiedenen Formaten (z. B. XRechnung oder ZUGFeRD) innerhalb des CRM-Systems. Dadurch können rechnungsbezogene Daten strukturiert verarbeitet, manuelle Arbeitsschritte reduziert und digitale Rechnungsprozesse effizienter sowie standardkonform abgebildet werden.
Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
Kunden Mitarbeiter Lieferanten Endnutzer
Kategorien personenbezogener Daten, die verarbeitet werden
Stammdaten und Kommunikationsdaten der Cloudworx-Konten von Kunden. IT-System-spezifische Daten, wie z.B. User-Name, Zugriffsrechte, IP-Adressen. Rechnungsdaten aus dem Salesforce-System des Kunden, z. B. Namen, Anschriften und Kontaktdaten von Rechnungsempfängern und Ansprechpartnern, Bankverbindungen sowie Rechnungspositionen.
Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangs-beschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
Sensible Kundendaten, die bei Erstellung der Dokumente durch den Service verarbeitet werden. Angewandte Beschränkungen und Garantien: Strenge Zweckbindung, Zugangsbeschränkungen, Zugang nur für Cloudworx-Mitarbeiter, die eine spezielle Schulung absolviert haben, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen.
Art der Verarbeitung
Berechnung, Verarbeitung, Speicherung, Synchronisation und andere Dienste, wie in der Dokumentation beschrieben und vom Kunden von Zeit zu Zeit veranlasst.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Erstellung, Auslesen und Validierung digitaler, maschinenlesbarer Rechnungen. Synchronisation mit Salesforce. Fernwartung, Service und Support.

Dauer der Verarbeitung
Entsprechend der Laufzeit des Hauptvertrages.
Verarbeitung durch (Unter-)Auftragsverarbeiter. Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Subunternehmer 1: Host Europe GmbH Gegenstand: Bereitstellung von Cloud-Infrastruktur für die temporäre Verarbeitung und Zwischenspeicherung von Kundendaten zur Erstellung elektronischer Dokumente. Art: Verarbeitung, temporäre Speicherung und Übermittlung von Daten des Kunden. Die Verarbeitung erfolgt ausschließlich zur technischen Bereitstellung der Dokumentenerstellung innerhalb von XRSF. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung. Temporär zwischengespeicherte Daten werden nur für die Dauer verarbeitet, die zur Erstellung und Bereitstellung der jeweiligen Dokumente erforderlich ist, und anschließend gemäß den festgelegten Löschprozessen gelöscht.
Subunternehmer 2: Scalyr, LLC (vormals Scalyr, Inc.; DataSet, Unternehmen der SentinelOne-Gruppe) Gegenstand: SaaS-Plattform für das Protokoll-Management und die Server-Überwachung. Art: Verarbeitung, Speicherung und Übermittlung von Protokolldaten des Kunden. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung.
Subunternehmer 3: Amazon Web Services EMEA SARL Gegenstand: Bereitstellung von Cloud-Infrastruktur für die temporäre Verarbeitung und Zwischenspeicherung von Kundendaten zur Erstellung elektronischer Dokumente. Art: Verarbeitung, temporäre Speicherung, Zwischenspeicherung und Übermittlung von Daten des Kunden auf Serverinfrastruktur in der AWS Region Europe (Frankfurt). Die Verarbeitung erfolgt ausschließlich zur technischen Bereitstellung der Dokumentenerstellung innerhalb von XRSF. Dauer: Entsprechend der Laufzeit des Hauptvertrages bzw. der Laufzeit der Service- und Supportvereinbarung. Temporär zwischengespeicherte Daten werden nur für die Dauer verarbeitet, die zur Erstellung und Bereitstellung der jeweiligen Dokumente erforderlich ist, und anschließend gemäß den festgelegten Löschprozessen gelöscht.

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

Gegenstand

Gegenstand dieser Anlage ist die Festlegung technischer und organisatorischer Maßnahmen zur Sicherstellung des Schutzes personenbezogener Daten.

Gem. Art. 32 DSGVO muss bei der Verarbeitung von personenbezogenen Daten sichergestellt sein, dass geeignete technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit, der Integrität, Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit der Daten eingerichtet sind und eingehalten werden. Die Verpflichtung der Auftragnehmerin geeignete Maßnahmen zum Schutz der personenbezogenen Daten zu treffen, erstreckt sich gem. Art. 32 Abs. 1 DSGVO nur auf solche Maßnahmen deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Über die eingerichteten, technischen und organisatorischen Maßnahmen ist ein Nachweis zu führen.

Das vorliegende Dokument fasst die von der Auftragnehmerin eingerichteten technischen und organisatorischen Maßnahmen zusammen. Es gilt für alle informationsverarbeitenden Systeme und Netzwerke, Dokumente und Informationen der Auftragnehmerin, mit denen personenbezogene Daten erhoben, verarbeitet, genutzt und gespeichert werden. Es bezieht sich sowohl auf Daten in Papierform wie auch auf Daten, die digital verarbeitet werden.

1. Allgemeines

Die cloudworx GmbH hat sichergestellt, dass

- ein schriftliches oder elektronisches Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO geführt wird,
- ein Datenschutzmanagementsystem etabliert ist, das die Anforderungen der DSGVO erfüllt,
- ein Datenschutzverantwortlicher benannt ist, der die Einhaltung der datenschutzrechtlichen Anforderungen sicherstellt,
- die Mitarbeiter durch regelmäßige Schulungen über die Anforderungen des Datenschutzes und die zu treffenden technischen und organisatorischen Maßnahmen unterrichtet werden,
- die Mitarbeiter, die mit der Verarbeitung der personenbezogenen Daten beschäftigt sind, zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
- ein Prozess zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO eingeführt ist.

2. Maßnahmen zur Pseudonymisierung und Verschlüsselung gem. Art. 32 Abs. 1 lit. a) DSGVO

- Gespeicherte Daten auf stationären oder mobilen Speichermedien der cloudworx GmbH (Data at Rest), wie z.B. Büro-PC, Notebooks, Tablets und externe Festplatten, sind nach dem Stand der Technik verschlüsselt.

- Gespeicherte Daten bei Cloud-Service-Providern (Data at Rest), sind ebenfalls nach dem Stand der Technik verschlüsselt.
- Daten, die sich in Übertragung befinden, z.B. im cloudworx-Netzwerk oder zwischen Cloud-Diensten, sind nach dem Stand der Technik verschlüsselt.
- Das WLAN der cloudworx GmbH ist nach dem Stand der Technik verschlüsselt.
- Bei der Kommunikation mit der Webseite der cloudworx GmbH werden die übertragenen Daten mittels einer Transportverschlüsselung nach dem Stand der Technik verschlüsselt.

3. Maßnahmen zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Gewährleistung der Belastbarkeit der Systeme und Dienste gem. Art. 32 Abs. 1 lit. b) DSGVO

Zutrittskontrolle

Unter „Zutritt" ist der physische Zugang von Personen zu Räumen und Gebäuden zu verstehen, in denen IT-Systeme betrieben und/oder genutzt werden. Dazu gehören z.B. Rechenzentren, in denen Web-Server, Applikationsserver, Datenbanken, Speichersysteme betrieben werden und Räumlichkeiten, in denen sich Infrastrukturkomponenten für den Betrieb von Netzwerken, sowie die dazugehörigen Verkabelungen befinden. Ebenfalls dazu gehören Büroräume oder andere Arbeitsflächen, in denen Mitarbeiter die PC-Systeme nutzen.

Das Ziel der Zutrittskontrolle ist es, den unbefugten Zutritt zu Räumen bzw. unbefugte Nutzung von IT-Systemen, in bzw. mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verhindern.

- Die **Geschäftsräume** sind gegen unbefugten Zutritt gesichert. Die Türen der Geschäftsräume verfügen über Sicherheitsschlösser. Die Ausgabe von Schlüsseln erfolgt entsprechend einer Schlüsselregelung, die auch festlegt, unter welchen Umständen die Schlüssel zurückgegeben werden müssen. Es existiert ein Nachweis über die ausgegebenen Schlüssel.
- In den Geschäftsräumen befinden sich **keine Räume für IT-Infrastruktur,** in denen die cloudworx GmbH ihre zentralen IT-Systeme (Server, Storage) oder Netzwerkinfrastrukturkomponenten betreibt.
- Die Verarbeitung personenbezogener Daten erfolgt über Cloud-Service-Provider, deren Services vor deren Beauftragung auf ihre DSGVO-Konformität geprüft wurden. Mit allen Anbietern wurden **Verträge zur Auftragsverarbeitung nach Art. 28 DSGVO** vereinbart. Der Zutritt zu diesen Räumen ist nur besonders berechtigten Personen, entsprechend den Regelungen der Cloud-Service-Provider gestattet. Die dort vereinbarten Zutrittsregelungen wurden geprüft oder sind durch Zertifizierungen belegt. Es besteht ein Auditrecht.
- Die **Türen** sind durch elektronische Schlösser gesichert, die mit einem automatischen Zutrittskontroll-system in Kombination mit elektronischen Ausweisen gesichert sind.
- **Besucher** dürfen die Geschäftsräume nur in Begleitung eines cloudworx-Mitarbeiters betreten.
- **Externe Dienstleister,** die sich außerhalb der Geschäftszeiten in den Geschäftsräumen aufhalten, wie z.B. Reinigungspersonal, werden sorgfältig ausgewählt.

Zugangskontrolle

Die Zugangskontrolle stellt sicher, dass ein IT-System nur von berechtigten Nutzern genutzt wird bzw. nur mit anderen autorisierten IT-Systemen kommuniziert. Die Zugangskontrolle umfasst auch das Verhindern des

unbefugten Zugriffs über externe Schnittstellen, wie z.B. Internetanschlüsse.

Das Ziel der Zugangskontrolle ist es, zu verhindern, dass IT-Systeme, die der Verarbeitung von personenbezogenen Daten dienen, von Unbefugten benutzt werden.

- Für **verschiedene Anwendungen und Dienste** werden unterschiedliche Passwörter verwendet. Die Passwörter werden, entsprechend dem Stand der Technik, in Passwortmanagern verwaltet. Sofern unterstützt, erfolgt die Anmeldung bei der Nutzung von Online-Diensten über eine Zwei-Faktor-Authentisierung.
- **Passwörter** sind an natürliche Personen gebunden und dürfen nicht weitergegeben werden.
- Die Vergabe von Passwörtern erfolgt entsprechend einer, an aktuellen Standards orientierten, **Passwortrichtlinie,** die regelmäßig überprüft und ggf. aktualisiert wird.
- **Kompromittierte Passwörter** müssen unverzüglich geändert werden.
- **Voreingestellte Passwörter, temporäre Passwörter, Passwörter im Auslieferungszustand** sowie automatisch vergebene Passwörter für Hard- und Software müssen sofort geändert werden.
- Einzelnen Mitarbeitern individuell zugewiesene Accounts müssen nach deren Ausscheiden unverzüglich insgesamt deaktiviert werden.
- Sofern die betreffende Anwendung eine dahingehende Konfiguration erlaubt, sollen häufige, fehlgeschlagene Anmeldeversuche zu zeitlichen **Sperrungen** führen.

Zugriffskontrolle

Die Zugriffskontrolle ist die bedarfsgerechte Planung, Steuerung und Überwachung des Zugriffs auf IT-Ressourcen. Wesentliche Punkte der Zugriffskontrolle sind ein angemessenes Berechtigungskonzept für die Vergabe, Änderung und den Entzug von Zugriffsrechten, sowie dessen Überwachung und Protokollierung.

Das Ziel der Zugriffskontrolle ist es, sicherzustellen, dass die Zugriffsberechtigten ausschließlich auf die freigegebenen Daten zugreifen können.

- Bei der Vergabe von Benutzerrechten und Programmberechtigungen ist sichergestellt, dass die Berechtigten nur die zur Erledigung ihrer Aufgaben notwendigen Berechtigungen erhalten (**Need-to-know-Prinzip**). Die Vergabe basiert auf einem **Berechtigungskonzept**, dessen Rollen und Rechte regelmäßig überprüft und angepasst werden. Die zugewiesenen Rollen und die vergebenen Rechte werden regelmäßig überprüft und sofern erforderlich angepasst.
- **Administratorenrechte** werden nur soweit erforderlich ausgewählten Mitarbeitern zugewiesen. Die Anmeldung mit Administratorrechten ist nur für die Installation von Software, bei Konfigurationsänderungen und für den Betrieb der Kundenservices möglich.
- **Externe Dienstleister** haben keinen Zugriff auf IT-Systeme oder Telekommunikationseinrichtungen von cloudworx. Sofern Dienstleister Supportaufgaben erfüllen, z.B. 3rd Level-Support, erfolgt der Zugriff nur im Rahmen von beaufsichtigten Supportsitzungen.
- Damit kein unbefugter Zugriff erfolgen kann, werden **Arbeitsplatzrechner** beim Verlassen des Raums gesperrt. Für die Arbeitsplatzrechner ist eine automatische Bildschirmsperre aktiviert. Bei Bedarf kann die Bildschirmsperre auch manuell aktiviert werden.
- Die Bildschirme der Rechner sind so platziert, dass die **Bildschirminhalte** vor fremden Blicken geschützt sind.

- Nicht benötigte **Netzwerk-Ports** sind deaktiviert.
- Es existiert ein **Löschkonzept**. Datenträger werden nach den Vorgaben der DIN 66399 gelöscht. Wenn Akten bzw. Datenträger durch cloudworx oder einen beauftragten Dienstleister vernichtet und dabei physisch zerstört werden, erfolgt die Vernichtung entsprechend der Vorgaben der DIN 66399.

Integrität

Die Integrität ist die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von IT-Systemen.

Das Ziel der Integrität ist es, die Korrektheit der Daten sowie die korrekte Funktionsweise der IT-Systeme sicherzustellen.

- Das gesamte Netzwerk der cloudworx GmbH ist durch eine anforderungsgerecht konfigurierte und regelmäßig aktualisierte **Firewall** geschützt.
- Alle Endgeräte sind durch ein **Virenschutzprogramm** geschützt, dessen Virensignaturen regelmäßig aktualisiert werden. Datenträger und Dienste, die eine Übermittlung von Dateien von Dritten, z.B. von E-Mail-Anhängen, ermöglichen, werden überwacht. Empfangene Dateien werden vor dem Öffnen überprüft.
- Empfangene E-Mails werden auf **Spam und Schadsoftware** überprüft.
- Für Gäste wird ein Internetzugang über ein separates, dafür vorgesehenes **Gäste-WLAN** bereitgestellt.
- **Private Mitarbeitergeräte** werden nicht für die Verarbeitung von personenbezogenen Daten der Kunden verwendet.
- Die verwendeten Betriebssysteme der Endgeräte werden vom Hersteller unterstützt. Die von Herstellerseite bereitgestellten, **regelmäßigen Updates** werden installiert. Die von den Herstellern bereitgestellten Sicherheits-Updates (insbesondere für Virenschutzprogramme, Office-Anwendungen und zentrale IT-Systeme wie Firewall, Router etc.) werden regelmäßig überprüft und installiert.
- Von externen Quellen bereitgestellte Dokumente werden vor dem Öffnen auf **Schadsoftware** überprüft. In Office-Anwendungen werden nur überprüfte und digital signierte Makros aktiviert, sofern dies technisch möglich ist und die weiteren Systeme und Software ohne Einschränkungen verwendet werden können.
- Die Mitarbeiter werden regelmäßig in angemessenem Umfang zu Fragen der IT-Sicherheit und der Sicherheit der Verarbeitung personenbezogener Daten qualifiziert und sensibilisiert. Dabei wird insbesondere über die Gefahren durch externe Inhalte, etwa durch das ungeprüfte Öffnen von Dateianhängen und Links, informiert.

Verfügbarkeit

Die Verfügbarkeit bezeichnet die Wahrscheinlichkeit, dass ein IT-System oder ein Dienst zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand anzutreffen ist.

Das Ziel der Verfügbarkeit ist es, dass ein System oder ein Dienst für die berechtigte Person zu dem vorgesehenen Zeitpunkt zur Verfügung steht und die korrekte Funktionsweise gewährleistet ist.

- Die **Hardware** der cloudworx GmbH wird regelmäßig gewartet und unter Berücksichtigung des Standes der Technik erneuert.
- Die IT-Systeme und Services der Cloud Service Provider (Server, Storage) sind vor den wesentlichen

Umgebungs- und Elementarrisiken (Luftfeuchtigkeit, Staubbelastung, Temperatur, Feuer, Wasser etc.) geschützt und verfügen über eine redundante Infrastruktur (Strom, Internet).

- Daten werden **nicht lokal** auf den Arbeitsplatzrechnern gespeichert, sondern in Cloud-Umgebungen, die über Backup gesichert werden.
- Bei **Fernwartung** wird ein Protokoll erstellt, so dass nachvollziehbar ist, welche Veränderungen vorgenommen wurden und wer auf welche Daten zugegriffen hat. Die Fernwartung erfolgt über eine verschlüsselte Verbindung.
- Damit Abhängigkeiten von der Verfügbarkeit von Systemkomponenten oder IT-Services vermieden werden, setzt cloudworx auf offene Standards, die von mehreren Herstellern bzw. Cloud Service Providern bezogen werden können (Vermeidung von Lock-in-Effekten).

Belastbarkeit (Resilience)

Die Belastbarkeit, in der englischen Version der DSGVO als „resilience“ bezeichnet, ist die Widerstandsfähigkeit eines IT-Systems oder Dienstes, trotz massiver externer oder interner Störungen wieder in den Ausgangszustand zurückzukehren. Ein technisches System wird als resilient bezeichnet, wenn das System seine Leistung trotz einer internen oder externen Störung erbringt und den Systembetrieb aufrechterhält.

Das Ziel der Widerstandsfähigkeit ist die Aufrechterhaltung der Funktionsfähigkeit, um die Verarbeitung personenbezogener Daten wie vorgesehen ordnungsgemäß durchführen zu können.

- Die cloudworx GmbH stellt die Resilienz der IT-Services mit Hilfe einer SaaS-Lösung für das Protokollmanagement und die Server-Überwachung sicher.
- Für die Sicherstellung der Leistungsfähigkeit der IT-Services werden Cloud Services genutzt, die bei steigender Last die Arbeit auf eine größere Anzahl von Servern verteilen.

4. Maßnahmen für die rasche Wiederherstellung der Verfügbarkeit der Daten und des Zugangs zu ihnen bei einem Zwischenfall gem. Art. 32 Abs. 1 lit. c) DSGVO

Die Wiederherstellung der Verfügbarkeit und des Zugangs zu Daten bezeichnet die Wiederherstellung von Originaldaten nach einem Datenverlust aus einer Sicherungskopie sowie auch die Erkennung fehlerhaft übertragener Dateneinheiten und deren Wiederherstellung im weiteren Sinne.

Das Ziel der Wiederherstellung ist es, die Originaldaten verfügbar zu machen, damit die Verarbeitung personenbezogener Daten wie vorgesehen ordnungsgemäß stattfinden kann.

- Die cloudworx GmbH hat ein Notfall-Konzept erstellt, in dem festgelegt ist, wer unter welchen Umständen Maßnahmen zur Wiederherstellung der IT-Services einleitet. Die dafür erforderlichen Informationen, wie z.B. Zugangsdaten, Passwörter, Authentifizierungsinformationen, Ansprechpartner und Kontaktdaten sind dokumentiert und sicher gespeichert.
- Die cloudworx GmbH hat ein Backup-Konzept erstellt und umgesetzt. In dem Backup-Konzept ist
  - die Zuständigkeit für das Backup geregelt,
  - festgelegt, dass das Backup sämtliche Daten umfasst,
  - festgelegt, dass das Backup nach der sog. 3-2-1-Regel erfolgt,
  - festgelegt, dass das Backup regelmäßig auf Vollständigkeit, Korrektheit und Wiederherstellbarkeit geprüft wird.

- Die Backupmedien und der Datenübertragungsweg sind nach dem Stand der Technik verschlüsselt.

5. Kontrolle der vorgenannten Maßnahmen gem. Art. 32 Abs. 1 lit. d) DSGVO

- Die cloudworx GmbH überprüft die Maßnahmen regelmäßig, in der Regel jährlich oder wenn ein konkreter Anlass besteht, auf ihre Einhaltung und Wirksamkeit.
- Die cloudworx GmbH hat eine Dokumentation der IT-Infrastruktur, einschließlich eines Netzwerkplans, erstellt. Die IT-Dokumentation wird regelmäßig, in der Regel jährlich, oder wenn ein konkreter Anlass besteht, überprüft und ggf. aktualisiert.

Anhang IV - Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Unterauftragsverarbeiter		**Kontaktperson**			**Verarbeitung**
Name	Anschrift	Name	Funktion	Kontaktdaten	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden).
Salesforce, Inc.	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA	Salesforce Data Protection Officer (Salesforce Privacy Team) 415 Mission St, 3rd Floor San Francisco, CA 94105, USA		Web-Service: www.salesforce.com/form/other/privacy-request/ E-Mail: privacy@salesforce.com Phone: 1-844-287-7147	Bereitstellung einer SaaS-Lösung für das Projektmanagement.
Host Europe GmbH	Hansestrasse 111 51149 Köln, Deutschland	RA Dr. Karsten Kinast	Daten-schutz-beauf-tragter	E-Mail: mail@kinast.eu Tel.: +49 221 222183-0	Speicherung und Backup von Kundendaten.
Scalyr, LLC (vormals Scalyr, Inc.; DataSet, Unternehmen der SentinelOne-Gruppe)	c/o SentinelOne, Inc., 444 Castro Street, Suite 400, Mountain View, CA 94041, USA	SentinelOne Privacy Team	Data Protection Officer	E-Mail: privacy@sentinelone.com	Betrieb einer SaaS-Lösung für das Protokollmanagement und die Server-Überwachung.
Twilio Ireland Limited,	25-28 North Wall Quay Dublin 1, Ireland	Twilio Privacy Team		E-Mail: privacy@twilio.com	Bereitstellung eines Dienstes für die Übermittlung von Kurznachrichten.
finAPI GmbH	Adams-Lehmann-Str. 44	finAPI GmbH zu Hd. Abteilung Datenschutz		E-Mail: datenschutz@finapi.io	Bereitstellung einer Schnittstelle für die Übermittlung von

	80797 München, Deutschland	Adams-Lehmann-Str. 44 80797 München, Deutschland		Finanzinformationen.
Google LLC	1600 Amphitheatre Parkway Mountain View, CA 94043, USA	Google LLC Attn: Data Protection 1600 Amphitheatre Pkwy Mountain View CA 94043 United States of America	Tel.: +1 650 253 0000	Bereitstellung einer cloud-basierten Lösung für die Kommunikation und Zusammenarbeit sowie zugehöriger Apps für das Erstellen von Textdokumenten, Tabellenkalkulationen und Präsentationen (Google Workspace).
Dropbox, Inc.	333 Brannan Street, San Francisco, CA 94107, USA		https://www.dropbox.com	Bereitstellung eines Cloud-Dienstes für die Speicherung und den Austausch von Daten.
Spanning Cloud Apps, LLC	501 Congress Ave, Ste 200, Austin, TX 78701, USA		E-Mail: privacy @spanning.com	Bereitstellung eines Cloud-Dienstes für die Sicherung und Wiederherstellung von Daten.
Doxis AI Solutions B.V. (vormals Klippa App B.V.)	Laan Corpus Den Hoorn 1 9728 JM Groningen Die Niederlande		Tel.: +44 330 828 0642 E-Mail: support@klippa.com	Bereitstellung von Schnittstellen für die Verarbeitung von Dokumenten zur Auslesung mit Hilfe von künstlicher Intelligenz (KI).
Hypatos GmbH	Hypatos GmbH, c/o Office Club Am Neuen Markt 9 E-F 14467 Potsdam Germany	Proliance GmbH / www.datenschutzexperte.de Datenschutzbeauftragter Leopoldstr. 21 80802 München datenschutzbeauftragter@datenschutzexperte.de	Tel.: +49 (0) 302 09 97 00 info@hypatos.ai	Bereitstellung von Schnittstellen für die Verarbeitung von Dokumenten zur Auslesung mit Hilfe von künstlicher Intelligenz (KI).
Natif.ai GmbH	Campus Starterzentrum Gebäude A1 1	natif.ai GmbH Managing director: Johannes Korves Campus Starterzentrum	E-Mail: contact@natif.ai	Bereitstellung von Schnittstellen für die Verarbeitung von Dokumenten zur

	66123 Saarbrücken Germany	Gebäude A1 1 66123 Saarbrücken Germany		Auslesung mit Hilfe von künstlicher Intelligenz (KI).
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg, Luxemburg	Data Protection Officer / AWS Privacy Team	E-Mail: aws-EU-privacy@amazon.com	Bereitstellung von Cloud-Infrastruktur für die temporäre Verarbeitung und Zwischenspeicherung von Kundendaten zur Erstellung elektronischer Dokumente. Die Verarbeitung erfolgt in der AWS Region Europe (Frankfurt) auf Serverinfrastruktur in Deutschland. Die Verantwortlichkeit von AWS beschränkt sich auf den Betrieb und die Bereitstellung der hierfür erforderlichen Cloud-Infrastruktur.