Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

Muster GmbH
Max Muster
Musterstraße 1
12345 Musterstadt
max.muster@muster-gmbh.de
– nachfolgend "Auftraggeber" genannt –

und

Auftragnehmer
– nachfolgend "Auftragnehmer" genannt –

gemeinsam auch "die Parteien" genannt.

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Im Einzelnen sind die Angaben in **Anlage 1** Bestandteil der Datenverarbeitung.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

2. Die Weisungen werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen gemäß **Anlage 4** zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Der Auftragnehmer unterrichtet den Auftraggeber über Verletzungen des Schutzes personenbezogener Daten des Auftraggebers spätestens innerhalb von 12 Stunden nach Kenntnisnahme. Die Meldung erfolgt über den definierten Kontaktweg: E-Mail an max.muster@muster-gmbh.de mit dem Betreff "DSGVO-Verletzung - Dringend" oder telefonisch unter der im Vertrag angegebenen Notfallnummer. Die Meldung muss mindestens folgende Informationen enthalten:
    - **Art der Verletzung:**Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (z.B. unbefugter Zugriff, Datenverlust, unberechtigte Weitergabe, Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit),
    - **Umfang der Verletzung:**Angaben zum Umfang der betroffenen Daten (Anzahl der Datensätze, Kategorien der betroffenen Daten, Zeitraum der Verletzung),
    - **Betroffenheit:**Beschreibung der betroffenen Personen (Kategorien und ungefähre Anzahl der betroffenen Personen, soweit möglich auch konkrete Angaben zu betroffenen Personen),
    - **Ergriffene Maßnahmen:**Beschreibung der bereits ergriffenen oder geplanten Maßnahmen zur Behebung der Verletzung und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Die Meldung hat alle Informationen zu enthalten, die erforderlich sind, damit der Auftraggeber seine Meldepflichten nach Art. 33 DSGVO (innerhalb von 72 Stunden nach Kenntnisnahme) erfüllen kann.

6. Der Auftragnehmer hat zur Klärung von Datenschutzfragen und zur Einhaltung der gesetzlichen Aufgaben nach der DS-GVO, dem BDSG (neu) und dem Hessischen Landesdatenschutzgesetz einen externen Datenschutzbeauftragten bestellt.

7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

11. Der Auftragnehmer benennt dem Auftraggeber in **Anlage 2** die Person(en), die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangsberechtigten Personen ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. Datenschutz-rechtlicher Bestimmungen feststellt.

2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 3 Abs. 10 entsprechend.

3. Der Auftraggeber nennt dem Auftragnehmer in **Anlage 2** den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, oder Auskunft an den Auftragnehmer, wird dieser die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter und unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
    - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
    - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
    - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
    - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

3. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

4. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder

Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb von zwei Wochen nach Mitteilung – aus einem datenschutzrechtlichen Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

2. Über die in **Anlage 3** aufgeführten Unterauftragnehmer wird mit Unterzeichnung dieses Vertrages die notwendige Information erteilt und Zustimmung seitens des Auftraggebers vorausgesetzt. Ergänzungen und Änderungen teilt der Auftragnehmer auf geeignete Weise mit. Aktualisierungsinformationen werden immer auch unter https://www.some-solutions.de/dsgvo-verarbeiter erfolgen.

3. Der Auftragnehmer wird mit Subunternehmen Vereinbarungen treffen und diesen dieselben Datenschutzpflichten auferlegen, die sich aus diesem Vertrag ergeben.

§ 8 Löschung und Rückgabe von Daten, Backup-Regelungen

1. **Löschfristen:**Nach Abschluss der vereinbarten Leistungen oder auf Anweisung des Auftraggebers hat der Auftragnehmer personenbezogene Daten nach den jeweils einschlägigen gesetzlichen Vorgaben zu löschen oder an den Auftraggeber zurückzugeben, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

2. **Ablauf der Löschung:**Die Löschung erfolgt nach den gesetzlichen Vorgaben und orientiert sich an Art und Notwendigkeit der jeweils beauftragten Dienstleistung.
    - Vernichtung physischer Datenträger nach datenschutzgerechten Standards (z.B. DIN 66399),
    - Backups werden in der Regel täglich erstellt; auf den Hosting-Servern werden Sicherungen alle 3 Tage gelöscht.

3. **Backup-Regelungen:**Der Auftragnehmer erstellt regelmäßige Backups der verarbeiteten Daten. Diese Backups werden entsprechend den vorgenannten Regelungen aufbewahrt und anschließend automatisch gelöscht. Die Backup-Daten werden verschlüsselt gespeichert und unterliegen denselben Sicherheitsmaßnahmen wie die Produktivdaten.

4. **Ausnahmen:**Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, sind entsprechend gesetzlicher Aufbewahrungspflichten zu sichern. Diese werden getrennt von den personenbezogenen Daten aufbewahrt und unterliegen den gesetzlichen Aufbewahrungsfristen (in der Regel 10 Jahre).

5. **Rückgabeoption:**Auf ausdrückliche Anweisung des Auftraggebers können Daten statt der Löschung auch in einem strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber zurückgegeben werden. Die Rückgabe erfolgt verschlüsselt und innerhalb von 14 Tagen nach Anweisung.

§ 9 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein

Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

4. Es gilt deutsches Recht.

5. Als Gerichtsstand wird, soweit gesetzlich zulässig, Eschwege vereinbart.

§ 10 Haftung und Schadensersatz

Auftraggeber und der Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Anlage 1:
Gegenstand und Dauer der Verarbeitung, Kategorien von Daten und betroffenen Personen, Art und Zweck der Datenverarbeitung

Anlage 2:
Weisungsberechtigte Personen und Datenschutzbeauftragter

Anlage 3:
Unterauftragnehmer mit Beschreibung der Leistungen / Teilleistungen

Anlage 4:
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (vgl. auch § 3 Abs. 2)

Erstellt am: 22.06.2026

Anlage 1 - Gegenstand der Verarbeitung

Für Kunden die unser Webhosting nutzen:

Gegenstand des Vertrages ist die Bereitstellung von Webhosting-Dienstleistungen sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. Im Rahmen dieses Vertrages hat der Kunde – je nach Tarif und vereinbartem Leistungsumfang – unter Nutzung u.a. z.B. eines Webservers, FTP-Servers oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch ConRat.

Im Zuge der Leistungserbringung von ConRat als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Kundes, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

Art der Daten und Kreis der Betroffenen

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Kunden sind folgende Datenarten: Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten.

Der Kreis der durch den Umgang mit den Daten Betroffenen umfasst: Kunden, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Handelsvertreter und Ansprechpartner.

Art und Zweck der Datenverarbeitung

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Parteien bestehenden Vertrag.

ConRat ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. ConRat ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. ConRat ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Soweit seitens ConRat eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind.

Für Kunden die unser Adventskalender / Gewinnspieltool nutzen:

Die ConRat WebSolutions GmbH stellt dem Auftraggeber eine digitale Adventskalender-Plattform zur Verfügung. Diese umfasst die Bereitstellung, den Betrieb und die Wartung der Adventskalender-Anwendung sowie die damit verbundenen Dienstleistungen.

Art der Daten und Kreis der Betroffenen

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Kunden sind folgende Datenarten: Personenstammdaten (Name, E-Mail-Adresse), Kommunikationsdaten, Teilnahmedaten (Kalendertür-Öffnungen, Gewinnspiel-Teilnahmen), Nutzungsdaten der Plattform, Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten sowie technische Daten (IP-Adressen, Log-Daten).

Der Kreis der durch den Umgang mit den Daten Betroffenen umfasst: Kunden, Interessenten, Teilnehmer am Adventskalender, Gewinnspiel-Teilnehmer, Beschäftigte, Lieferanten, Handelsvertreter und Ansprechpartner.

Art und Zweck der Datenverarbeitung

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Parteien bestehenden Vertrag. Die Verarbeitung erfolgt insbesondere zur Bereitstellung, zum Betrieb und zur Wartung der Adventskalender-Plattform sowie zur Durchführung von Gewinnspielen und Marketing-Maßnahmen im Rahmen des Adventskalenders.

ConRat ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. ConRat ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. ConRat ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Soweit seitens ConRat eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind.

Für Kunden die unsere All-in-One KI-Plattform ConRat-AI nutzen:

1. Gegenstand und Geltungsbereich

Die ConRat WebSolutions GmbH stellt dem Auftraggeber eine KI-basierte Anwendungsplattform (ConRat AI) unter conrat-ai.de zur Verfügung. Diese Ergänzung informiert gemäß Art. 13, 14 DSGVO über die Verarbeitung personenbezogener Daten bei der Nutzung der KI-gestützten Funktionen und ergänzt die allgemeine Datenschutzerklärung unter conrat-ai.de/privacy.

Die KI-Dienste umfassen:

- KI-Chat (Text-Konversation mit verschiedenen Sprachmodellen)
- KI-Bildgenerierung
- Dokumenten-Chat (PDF-Analyse)
- RechercheMeister (KI-gestützte Webrecherche)

2. Kategorien verarbeiteter Daten

Bei der Nutzung der KI-Dienste werden folgende Datenkategorien verarbeitet:

- **Bestandsdaten:**E-Mail-Adresse, Benutzername, Kontoinformationen (gespeichert auf eigenem Server in Deutschland).
- **Nutzungsdaten:**Zeitpunkt der Nutzung, gewähltes KI-Modell, Credit-Verbrauch, Einwilligungsstatus je Dienst inkl. Zeitstempel und Version.
- **Inhaltsdaten (KI-Chat):**Text-Eingaben (Prompts) und KI-generierte Antworten. Gesprächsverläufe werden ausschließlich in der eigenen Datenbank in Deutschland gespeichert. An die KI-Anbieter werden nur die für die jeweilige Anfrage erforderlichen Prompts per zustandsloser API-Schnittstelle übermittelt. Es werden keine dauerhaften Sitzungen bei den KI-Anbietern erstellt.
- **Inhaltsdaten (Bildgenerierung):**Text-Prompts und ggf. Referenzbilder. Generierte Bilder werden ausschließlich auf dem eigenen Server in Deutschland gespeichert. Es werden keine personenbezogenen Metadaten (Name, E-Mail o. Ä.) an die KI-Anbieter übermittelt.
- **Inhaltsdaten (Dokumenten-Chat):**Hochgeladene PDF-Dokumente und darauf bezogene Fragen. Verarbeitung und Speicherung erfolgen ausschließlich in Deutschland (Frankfurt).
- **Inhaltsdaten (RechercheMeister):**Suchanfragen, die an die Perplexity Sonar API übermittelt werden. Suchanfragen können inhaltlich personenbezogene Daten enthalten. Es werden keine Account-Daten oder Dokumente an Perplexity übermittelt.

Der Kreis der durch den Umgang mit den Daten Betroffenen umfasst: Kunden, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Handelsvertreter, Ansprechpartner sowie Endnutzer der KI-Systeme.

3. Rechtsgrundlagen der Verarbeitung

- **Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):**Die Verarbeitung ist erforderlich zur Erbringung der vertraglich geschuldeten KI-Dienste.
- **Einwilligung (Art. 6 Abs. 1 lit. a DSGVO):**Vor der erstmaligen Nutzung jedes KI-Dienstes wird über einen Einwilligungsdialog die ausdrückliche Zustimmung eingeholt. Die Einwilligung ist jederzeit mit Wirkung für die Zukunft widerrufbar.
- **Einwilligung bei Drittlandtransfer (Art. 49 Abs. 1 lit. a DSGVO):**Soweit Daten in die USA übermittelt

werden (Claude Opus 4.5, Nano Banana Pro, RechercheMeister), erfolgt dies auf Grundlage der ausdrücklichen Einwilligung nach vorheriger Information über die damit verbundenen Risiken.

4. KI-Chat: Modelle und Verarbeitungsorte

Der KI-Chat bietet 8 verschiedene Sprachmodelle. 7 von 8 Modellen verarbeiten innerhalb der EU bzw. in Deutschland.

Modell	Plattform	Standort	Region	DSGVO
GPT-5 Mini	Microsoft Azure	Frankfurt, Deutschland	DE	Konform
GPT-4.1	Microsoft Azure	Frankfurt, Deutschland	DE	Konform
Llama 4 Maverick	Microsoft Azure	Frankfurt, Deutschland	DE	Konform
DeepSeek R1	Microsoft Azure	Gävle, Schweden	EU	Konform
Mistral Large 3	Microsoft Azure	Gävle, Schweden	EU	Konform
GPT-5.4	Microsoft Azure	Gävle, Schweden	EU	Konform
Gemini 2.5 Flash	Google Vertex AI	St. Ghislain, Belgien	EU	Konform
Claude Opus 4.5	Microsoft Azure	Virginia, USA	USA	Drittland*

** Bei Auswahl von Claude Opus 4.5 erfolgt ein Datentransfer in die USA. Der Transfer ist abgesichert durch EU-Standardvertragsklauseln (SCCs) im Rahmen der Microsoft DPA sowie ergänzend durch das EU-U.S. Data Privacy Framework (DPF). Nutzer können alternativ eines der 7 EU/DE-Modelle verwenden.*

5. KI-Bildgenerierung: Modelle und Verarbeitungsorte

3 von 4 Modellen verarbeiten DSGVO-konform in der EU. Es werden ausschließlich Text-Prompts und ggf. Referenzbilder übermittelt – keine personenbezogenen Metadaten.

Modell	Plattform	Standort	Region	DSGVO
Nano Banana Flash	Google Vertex AI	St. Ghislain, Belgien	EU	Konform
GPT Image 1.5	Microsoft Azure	Gävle, Schweden	EU	Konform
FLUX.2 Pro	Microsoft Azure	Gävle, Schweden	EU	Konform
Nano Banana Pro	Google AI Studio	Global (USA)	USA	Drittland*

** Alle generierten Bilder werden ausschließlich auf dem eigenen Server in Deutschland gespeichert. Vor der ersten Nutzung wird ein Einwilligungsdialog mit Hinweis auf den jeweiligen Verarbeitungsort angezeigt.*

6. Dokumenten-Chat (PDF-Analyse)

Die gesamte Verarbeitung erfolgt ausschließlich in Deutschland:

- **KI-Modell:**GPT-4.1 auf Microsoft Azure, Region Germany West Central (Frankfurt).
- **Dokumentenspeicherung:**Hochgeladene Dokumente werden auf dem eigenen Server in Deutschland

gespeichert.

- **Zugriffskontrolle:**Jeder Nutzer sieht nur seine eigenen Dokumente. Download-URLs sind signiert und zeitlich begrenzt (1 Stunde Gültigkeit).
- **Drittlandtransfer:**Keiner. Sämtliche Verarbeitung findet in Deutschland statt.

7. RechercheMeister (KI-Webrecherche)

Der RechercheMeister nutzt die Perplexity Sonar API für KI-gestützte Webrecherche. Die Verarbeitung erfolgt in den USA.

- **Übermittelte Daten:**Ausschließlich Suchanfragen. Keine Account-Daten, Dokumente oder sonstigen personenbezogenen Metadaten.
- **Zero Data Retention:**Perplexity speichert weder Prompts noch Antworten über die Echtzeitverarbeitung hinaus.
- **Kein Modell-Training:**Anfragen werden nicht zum Training von KI-Modellen verwendet.
- **Auftragsverarbeitung:**DPA mit EU-Standardvertragsklauseln (SCCs, Modul 2), SOC 2 Type II-Zertifizierung.
- **Einwilligung:**Vor der ersten Nutzung wird ein Einwilligungsdialog mit Hinweis auf die US-Verarbeitung angezeigt.

8. Auftragsverarbeiter (Art. 28 DSGVO)

Mit allen nachfolgend genannten Dienstleistern bestehen Auftragsverarbeitungsverträge (AVV/DPA) gemäß Art. 28 DSGVO.

Auftragsverarbeiter	Einsatzbereich	Region	AVV/DPA
Microsoft Azure	KI-Chat, Dokumenten-Chat, Bildgenerierung	Frankfurt (DE), Gävle (SE), Virginia (USA)	Microsoft Products and Services DPA
Google Cloud (Vertex AI)	KI-Chat (Gemini), Bildgenerierung (Nano Banana Flash)	St. Ghislain, Belgien (EU)	Google Cloud Data Processing Addendum
Perplexity AI	RechercheMeister (Webrecherche)	USA (Zero Data Retention)	Perplexity DPA mit EU-SCCs (Modul 2)
IONOS SE	Hosting der Plattform und Datenbank	Deutschland	IONOS AVV

9. Datenübermittlung in Drittländer (Art. 44 ff. DSGVO)

Ein Datentransfer in die USA erfolgt nur, wenn der Nutzer sich aktiv für eines der folgenden Modelle oder Features entscheidet:

- **Claude Opus 4.5 (KI-Chat):**Microsoft Azure, Virginia, USA. Garantien: EU-SCCs im Rahmen der Microsoft DPA, ergänzend EU-U.S. Data Privacy Framework (DPF, Angemessenheitsbeschluss vom 10. Juli 2023).
- **Nano Banana Pro (Bildgenerierung):**Google AI Studio, globale Verarbeitung (inkl. USA). Garantien: Google Cloud DPA mit SCCs. Es werden nur Text-Prompts übermittelt.
- **RechercheMeister (Perplexity AI):**USA. Garantien: DPA mit EU-SCCs (Modul 2), Zero Data Retention, SOC 2 Type II.

10. Technische und organisatorische Maßnahmen (Zusammenfassung)

- **Transportverschlüsselung:**Alle Datenübertragungen erfolgen über TLS/HTTPS.
- **Serverseitige API-Aufrufe:**API-Schlüssel werden ausschließlich serverseitig verarbeitet, kein Exposure im Browser.
- **Zustandslose Architektur:**Keine dauerhaften Sitzungen oder Threads bei den KI-Anbietern.
- **Eigene Datenhaltung:**Alle Gesprächsverläufe, Bilder und Dokumente werden ausschließlich auf dem eigenen IONOS-Server in Deutschland gespeichert.
- **Zugriffskontrolle:**Strikte Mandantentrennung – jeder Nutzer sieht nur seine eigenen Daten.
- **Kein KI-Training:**Kein KI-Anbieter verwendet Eingaben zum Trainieren von Modellen (vertraglich garantiert).
- **Abuse Monitoring:**Microsoft Azure prüft Anfragen automatisiert auf schädliche Inhalte ohne dauerhafte Speicherung der Nutzerdaten.

11. Einwilligungsmanagement

Vor der erstmaligen Nutzung jedes KI-Dienstes wird ein Einwilligungsdialog angezeigt, der den konkreten Verarbeitungsort und Anbieter sowie bei Drittlandtransfer einen ausdrücklichen Hinweis auf die US-Verarbeitung enthält. Die Einwilligung wird mit Zeitstempel und Versionsnummer dokumentiert und ist jederzeit widerrufbar.

12. Speicherdauer und Löschung

- **Gesprächsverläufe und generierte Inhalte:**Bis zur Löschung durch den Nutzer oder Kontolöschung.
- **Hochgeladene Dokumente:**Bis zur Löschung durch den Nutzer.
- **Daten bei KI-Anbietern:**Durch zustandslose API-Architektur und Zero-Data-Retention-Vereinbarungen keine dauerhafte Speicherung bei den KI-Anbietern.
- **Einwilligungsdaten:**Für die Dauer des Nutzerverhältnisses (Nachweispflicht gemäß Art. 7 Abs. 1 DSGVO).

ConRat ist verpflichtet, die zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. ConRat ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Für Kunden die unsere Chat- und Werbeplattform ChatBot4You nutzen:

Die ConRat WebSolutions GmbH stellt dem Auftraggeber eine digitale Werbe- und Chatplattform ChatBot4You zum direkten Kunden- und Interessentenkontakt bereit.

Kategorien von Daten und betroffenen Personen, Art und Zweck der Datenverarbeitung

Verarbeitete Daten sind anwendungsseitig Kontaktdaten, Kommunikationsdaten und -inhalte, Rechnungsdaten, sowie IP-Adressen und ggf. Passwörter für Accounts.

Zu den Kategorien der Betroffenen gehören der Auftraggeber (ggf. seine Mitarbeiter), Kunden des Auftraggebers, sowie Interessenten.

Die ConRat WebSolutions GmbH stellt die Anwendungsplattform bereit, erfasst, speichert und verarbeitet personenbezogene Daten im Auftrag des Auftraggebers, soweit Angebote durch diesen eingestellt und von Interessenten/Kunden eine Rückmeldung gegeben wird. Die ConRat WebSolutions GmbH ist an dieser Stelle Mittler und technischer Betreuer zwischen Endkunden und Auftraggeber.

Art und Zweck der Datenverarbeitung

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Parteien bestehenden Vertrag.

ConRat ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. ConRat ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. ConRat ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Soweit seitens ConRat eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind.

Erstellt am: 22.06.2026

Anlage 2 - Weisungsberechtigte Personen und Datenschutzbeauftragter

Weisungsberechtigte Personen des Auftraggebers:
siehe Angaben zum Kunden (Ansprechpartner)

Weisungsberechtigte Personen des Auftragnehmers:
Herr Matthias Steube, ConRat WebSolutions GmbH

Datenschutzbeauftragter/Ansprechpartner der ConRat GmbH
Externer DSB: PadPort Datenschutz
E-Mail: info@dsb-mitte.de
Telefon: 0152 29283797

Erstellt am: 22.06.2026

Anlage 3 - Unterauftragnehmer

Stand: 22.06.2026

Die nachfolgende Liste der Unterauftragnehmer ist Bestandteil dieser Vereinbarung. Änderungen und Ergänzungen werden dem Auftraggeber mitgeteilt. Der Auftraggeber kann der Änderung – innerhalb von zwei Wochen nach Mitteilung – aus einem datenschutzrechtlichen Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben.

Die Auflistung der eingesetzten Unterauftragnehmer kann sich von Zeit zu Zeit ändern. Die jeweils aktuelle Übersicht ist auf unserer Website unter https://www.some-solutions.de/dsgvo-verarbeiter abrufbar. Wir empfehlen, diese Seite in regelmäßigen Abständen einzusehen.

- domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning Deutschland
für das Webhosting unserer öffentlich zugänglichen Seite, sowie für das Webhosting des Kundenbereichs und für den Betrieb eines Mailservers
(TOM: https://www.df.eu/fileadmin/user_upload/DF_TOMs_DSGVO_V1.5_Deutsch.pdf).

- IONOS SE, Elgendorfer Str. 57, 56410 Montabaur
für das Hosting der KI-Server
(TOM: https://www.ionos.de/terms-gtc/fileadmin/pdf/terms-gtc/DE/AVV/DE_AVV_TOM_v1.0.pdf).

- consentmanager GmbH, Eppendorfer Weg 183, 20253 Hamburg
für den Consent-Banner (Cookie-Banner).

Erstellt am: 22.06.2026

Anlage 4 - Technische und organisatorische Maßnahmen

Stand: 22.06.2026

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt.

Hinweis: Diese Maßnahmen unterliegen dem technischen Fortschritt und werden fortlaufend angepasst. Änderungen sind zulässig, sofern das vereinbarte Sicherheitsniveau nicht unterschritten wird. Der Auftraggeber wird über wesentliche Änderungen informiert.

1. Pseudonymisierung

Die vom Kunden in der Software eingegebenen sowie die vom System erhobenen Daten werden mit einer User-ID gespeichert. Diese ist ein Pseudonym für den jeweiligen Nutzer und lässt sich über eine Tabelle mit den eingetragenen Daten (mindestens E-Mail-Adresse) verknüpfen.

2. Verschlüsselung

Datenträger in den Geschäftsräumen mit personenbezogenen Daten werden entsprechend dem Stand der Technik verschlüsselt. Der Zugang zu Server-Systemen sowie die Datenübertragung zwischen einzelnen Servern erfolgt über verschlüsselte Verbindungen. Die Software ist durch den Kunden ausschließlich über verschlüsselte Internetverbindungen (https) nutzbar.

3. Gewährleistung der Vertraulichkeit Zutrittskontrolle

Einsatz einer Schliessanlage mit Zutrittsberechtigung. Besucher dürfen die Geschäftsräume nur in Begleitung berechtigter Mitarbeiter betreten. Die Zutrittskontrolle zum Rechenzentrum erfolgt auf Basis der technischen und organisatorischen Maßnahmen des Rechenzentrumsbetreibers DomainFactory GmbH sowie der IONOS SE.

4. Zugangskontrolle

Die Anmeldung an IT-Systemen erfolgt über mindestens 10-stellige Kennwörter mit Sonderzeichen, Ziffer und/oder Klein- /Großbuchstaben. Sofern möglich sind die Login-Daten personenbezogen und nur dem jeweiligen Mitarbeiter bekannt. Die IT-Systeme sind durch eine Firewall gesichert. Für Remote-Zugriffe werden personenbezogene VPN-Zugänge genutzt.

5. Zugriffskontrolle

Für die Zugriffskontrolle sind differenzierte Berechtigungen nach dem Rollenkonzept eingerichtet. Die Freigabe von Daten erfolgt nur an berechtigte Personen. Zugewiesene Berechtigungen werden durch die Administratoren regelmäßig überprüft und bei Entfall der Notwendigkeit entzogen.

6. Trennungskontrolle

Soweit die betrieblichen Abläufe eine getrennte Verarbeitung und Auswertung von Daten ermöglichen wird diese entsprechend eingerichtet. Produktiv- und Testsysteme nutzen generell getrennte Datenbanken. Für Kundendaten

erfolgt eine logische Trennung auf Datenbankebene. Der Zugriff auf Produktivsysteme wird soweit wie möglich eingeschränkt.

7. Gewährleistung der Integrität Weitergabekontrolle

Zur Übertragung von Daten werden verschlüsselte Verbindungen entsprechend dem Stand der Technik eingesetzt. Die Remote-Einwahl in das interne Netzwerk erfolgt über VPN-Verbindungen.

8. Eingabekontrolle

Eingaben, Änderungen und Löschung von Produktivdaten sind nur durch Administratoren möglich.

9. Gewährleistung der Verfügbarkeit

Von Server-Systemen werden täglich Backups durchgeführt. Sicherungen werden zusätzlich räumlich getrennt an einem anderen Standort gespeichert. Auf allen Client-Rechnern ist Antiviren-Software installiert und wird fortlaufend aktualisiert. Die Gewährleistung der Verfügbarkeit auf Ebene des Rechenzentrums erfolgt darüber hinaus auf Basis der technischen und organisatorischen Maßnahmen des Rechenzentrumsbetreibers DomainFactory GmbH sowie der IONOS SE.

10. Gewährleistung der Belastbarkeit der Systeme

Um die Belastbarkeit der Systeme zu gewährleisten, setzen wir auf eine skalierbare Serverinfrastruktur und ein Monitoring um Trends und Lastspitzen zu erkennen und rechtzeitig darauf zu reagieren. Die Administratoren sind in der Lage, die unter 9. genannten Sicherungen zeitnah einzuspielen. Das Szenario wird in periodischen Abständen getestet.

11. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag. Sie sind in einer gesonderten Vereinbarung dem Datengeheimnis verpflichtet.

Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnamen wird mindestens jährlich durchgeführt. Dabei erfolgt auch eine Beurteilung der Angemessenheit des Schutzniveaus und gegebenenfalls eine Anpassung auf den aktuellen Stand der Technik, beispielsweise eine Umstellung auf neuere Verschlüsselungsverfahren.

Erstellt am: 22.06.2026