

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Zwischen der/dem

dem Kunden, der die JUMO Cloud nutzt⁽¹⁾

- Verantwortlicher - nachstehend Auftraggeber genannt -
und der/dem

JUMO GmbH & Co. KG
Moritz-Juchheim-Straße 1
36039 Fulda

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt,

wird folgende Vereinbarung über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 der EU
Datenschutz-Grundverordnung geschlossen:

(1) Elektronische Erfassung der individuellen Kundenanschrift

1. Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (im Folgenden „DSGVO“).

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz- Grundverordnung (im Folgenden DSGVO) zu verstehen.

In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Den Begriffen „Datenverarbeitung“ oder „Verarbeitung“ liegt die Definition i.S.d. Art. 4 Nr. 2 DSGVO zugrunde. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

(1) Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Hauptvertrag (Wartungsvertrag, Dienstleistungsvertrag etc.) oder jeweils erteilten Einzelaufträgen zur Erbringung von Dienstleistungen im Server-/Netzwerk-/Automatisierungs- oder Softwarebereich.

(2) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Hauptvertrages, des Einzelauftrages und dieses Auftragsverarbeitungsvertrages sowie nach Weisung des Auftraggebers verarbeiten.

(3) Die Verarbeitung erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags / Auftragsverhältnisses durch eine Partei.

3. Art und Zweck der Verarbeitung, Art der Daten, Kategorien betroffener Personen

Die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen der Datenverarbeitung ergeben sich aus der Anlage 1 (Details zur Verarbeitung) dieses Vertrages.

4. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- (3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- (4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- (5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.
- (6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
- (7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- (9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- (10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit ausdrücklicher Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5. Technisch-organisatorische Maßnahmen

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Es gelten die in Anlage 2 beschriebenen Einzelheiten).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

6. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- a) Eine Unterbeauftragung ist unzulässig.
 b) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
narz systems GmbH & Co. KG	36358 Herbstein/ Deutschland	Datenspeicherung und Support

- c) Die Auslagerung auf Unterauftragnehmer oder
 der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
 - Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
 - Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

- b) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.
- c) Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO ist einzuhalten. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 2) muss gewährleistet sein.

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Dies beinhaltet die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(5) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(6) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(7) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 9 dieses Vertrages muss gewährleistet sein.

9. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat

das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(5) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(6) 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, ISO 27001).

(7) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

10. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

11. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

12. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13. Sonstiges

(1) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. An die Stelle der unwirksamen Vereinbarung tritt eine Regelung, die dem Willen der Parteien am Nächsten kommt.

Fulda, 09.06.2020
Ort, Datum


Auftragnehmer

Die Einwilligung des Auftraggebers wird elektronisch erfasst.

Anlage 1 – Details der Verarbeitung

1. Art und Zweck der Datenverarbeitung

Die Datenverarbeitung dient folgendem Zweck:

Softwarewartung, Problembehebung, Benutzersupport, Einspielen von Updates / Upgrades, Konfigurationsanpassungen, Programmierarbeiten

2. Art der personenbezogenen Daten

Folgende Datenarten sind Gegenstand des Auftrags:

Allgemeine Daten / Kontaktinformationen

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Geschäftliche Kommunikationsdaten (z.B. Telefon, E-Mail, Firmenanschrift)
<input checked="" type="checkbox"/>	Private Kommunikationsdaten (z.B. Telefon, E-Mail, Privatanschrift)
<input type="checkbox"/>	Nationalität
<input type="checkbox"/>	Ausweisdaten / IDs (z.B. Pass, Führerschein, Sozialversicherungsnummer)
<input type="checkbox"/>	Geburtsdaten / Alter
<input type="checkbox"/>	(Personen-)Profile / Bilddateien
<input type="checkbox"/>	andere, bitte angeben:

Vertragsdaten

<input checked="" type="checkbox"/>	Allgemeine Vertragsdaten
<input type="checkbox"/>	Abrechnungs- und Zahlungsdaten
<input type="checkbox"/>	Bankverbindungsdaten / Kreditkartendaten
<input type="checkbox"/>	Vertrags-/ Nutzungshistorien
<input type="checkbox"/>	andere, bitte angeben:

Bonitätsdaten

<input type="checkbox"/>	Zahlungsverhalten
<input type="checkbox"/>	Scorewerte
<input type="checkbox"/>	Vermögensinformationen
<input type="checkbox"/>	andere, bitte angeben:

Berufliche Daten

<input type="checkbox"/>	Stammdaten
<input type="checkbox"/>	Lohn-/Gehaltsdaten / Einkommen
<input type="checkbox"/>	Qualifikationen / Entwicklungspotentiale / Berufsprofile
<input type="checkbox"/>	Gesundheits- / Sozialdaten
<input type="checkbox"/>	Arbeitszeitdaten
<input type="checkbox"/>	Reisebuchung /-abrechnungsdaten
<input type="checkbox"/>	Workflows
<input type="checkbox"/>	andere, bitte angeben:

Besondere Kategorien personenbezogener Daten

<input type="checkbox"/>	Rassische / Ethnische Herkunft
<input type="checkbox"/>	Politische Meinungen
<input type="checkbox"/>	religiöse / weltanschauliche Überzeugungen
<input type="checkbox"/>	Gewerkschaftszugehörigkeit
<input type="checkbox"/>	Genetische Daten
<input type="checkbox"/>	Biometrische Daten
<input type="checkbox"/>	Gesundheitsdaten
<input type="checkbox"/>	Daten zum Sexualleben / zur sexuellen Orientierung
<input type="checkbox"/>	Straftaten, Verurteilungen und Urteile
<input type="checkbox"/>	andere, bitte angeben:

Dienste- und IT-(Nutzungs) Daten

<input checked="" type="checkbox"/>	Gerätekennungen
<input checked="" type="checkbox"/>	Zugangsdaten
<input checked="" type="checkbox"/>	Identifikationsdaten / IDs
<input checked="" type="checkbox"/>	Telekommunikationsdaten / Nachrichteninhalte
<input checked="" type="checkbox"/>	Nutzungs- und Verbindungsdaten / Metadaten
<input checked="" type="checkbox"/>	Bild- / Videodaten
<input checked="" type="checkbox"/>	Audio- / Sprachdaten
<input type="checkbox"/>	andere, bitte angeben:

Fahrzeug-, Standort- und Kontextdaten

<input type="checkbox"/>	Fahrzeugkennungen / Fahrzeugidentifikationsdaten / FIN
<input type="checkbox"/>	Fahrzeug- / Fahrzeugzustands- / Fahrzeuganalysedaten
<input type="checkbox"/>	Kontext- und Umgebungsinformationen
<input type="checkbox"/>	Standort-/ standortbezogene Daten / Bewegungsdaten
<input type="checkbox"/>	andere, bitte angeben:

3. Kategorien der betroffenen Personen

Folgende Kategorien von Personen sind durch die Datenverarbeitung betroffen:

<input checked="" type="checkbox"/>	Kunden
<input checked="" type="checkbox"/>	Interessenten
<input type="checkbox"/>	Abonnenten
<input checked="" type="checkbox"/>	Dienstnutzer
<input checked="" type="checkbox"/>	Mittelbar Betroffene / Personen im Umfeld / Insassen
<input type="checkbox"/>	Besucher
<input type="checkbox"/>	Veranstaltungsteilnehmer
<input checked="" type="checkbox"/>	Kommunikationsteilnehmer
<input type="checkbox"/>	Bewerber
<input checked="" type="checkbox"/>	Mitarbeiter
<input checked="" type="checkbox"/>	ehemalige Mitarbeiter
<input checked="" type="checkbox"/>	Auszubildende / Praktikanten
<input type="checkbox"/>	Angehörige von Mitarbeitern
<input type="checkbox"/>	Gesellschafter / Organe
<input type="checkbox"/>	Geschäftspartner
<input type="checkbox"/>	Lieferanten und Dienstleister
<input type="checkbox"/>	Berater
<input checked="" type="checkbox"/>	Dienstliche Ansprechpartner
<input type="checkbox"/>	Handelsvertreter
<input type="checkbox"/>	Pressevertreter
<input type="checkbox"/>	andere, bitte angeben:

Anlage 2 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
kein unbefugter Zutritt zu Datenverarbeitungsanlagen:
 - persönliche Transponder
 - elektronische Türöffner an den selbstverschließenden Außentüren
 - Anwesenheitsaufzeichnungen von Mitarbeitern sowie Besuchern
 - Dokumentierte und nachprüfbare Schlüsselregelung
 - Einbruchmeldeanlage sowie Kameraaufzeichnungen
 - Zutritt zu Rechenzentren nur für autorisierte Personen
- **Zugangskontrolle**
keine unbefugte Systembenutzung:
 - personalisierte Benutzerkonten
 - sichere Kennwörter, soweit möglich Zwei-Faktor-Authentifizierung
 - automatische Sperrmechanismen
 - Verschlüsselung von mobilen Datenträgern
- **Zugriffskontrolle**
kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte sowie Protokollierung von Zugriffen
- **Trennungskontrolle**
getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch Mandantenfähigkeit

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
- **Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-

Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfall bzw. Wiederanlaufpläne

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Vorfalls-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle, durch:
 1. Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO
 2. Weisungsbefugnisse sind festgelegt
 3. Bestellung eines Datenschutzbeauftragten seitens des Auftragsverarbeiters
 4. Sicherstellung der Rückgabe und/oder Vernichtung von Daten nach Beendigung des Auftrags