

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt

und

visoma gmbh, Hambrocker Str. 49, 29525, Uelzen, Deutschland

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Gegenstand des Auftrags ist die Erbringung von IT-Dienstleistungen und die Bereitstellung von IT-Services und Software für den Auftraggeber.

(2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 14 Tagen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

- a) Individuelle Softwareentwicklung, -pflege, -wartung und -support für den Auftraggeber
- b) Softwareentwicklung, -pflege, -wartung und -support der Standardsoftware "visoma tickets" für den Auftraggeber
- c) Softwareindividualisierung, -pflege, -wartung und -support der Standardsoftware "Bitrix24" für den Auftraggeber
- d) Wartung und Support der IT Umgebung des Auftraggebers
- e) Einrichtung, Wartung und Support von Cloud IT Services

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Art der Daten/ Kategorien betroffener Personen

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

Kommunikationsdaten (z.B. Telefon, E-Mail)

Kundenhistorie

Personenstammdaten

Planungs- und Steuerungsdaten

Vertragsabrechnungs- und Zahlungsdaten

Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Ansprechpartner

Beschäftigte

Interessenten

Kunden

Lieferanten

4. 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 [Einzelheiten in Anlage 1].

(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.

5. 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.

6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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:

- 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.
 - Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.
- 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 1].
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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.
- 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.
- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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.

- 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:

Eine regelmäßig aktualisierte Liste der Unterauftragnehmer ist zu finden unter:
www.visoma.de/adv

(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 bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. Kontrollrechte des Auftraggebers

(1) 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.

(2) 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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

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

9. 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.

- 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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- 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
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- 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.

10. 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.

11. 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.

Datum

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Verantwortliche Stelle

Firma	visoma gmbh
Straße	Hambrocker Str. 49
PLZ/Ort	29525 Uelzen
Telefon	0581-2115290- 0
Fax	0581-2115290- 21
E-Mail	office@visoma.de
Internet Adresse (URL)	https://www.visoma.de
Fachverantwortlicher für dieses Verfahren	Mike Bergmann
Organisationseinheit	Geschäftsführung

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

- Zutrittskontrolle:
 - Alarmanlage
 - Manuelles Schließsystem
 - Schlüsselregelung/Schlüsselbuch
 - Sicherheitsschlösser
 - Personenkontrolle beim Empfang
- Zugangskontrolle:
 - Authentifikation mit Benutzer+Passwort
 - Benutzerberechtigungen verwalten
 - Einsatz von Anti-Viren-Software
 - Einsatz von Firewalls
 - Einsatz von VPN-Technologie
 - Erstellen von Benutzerprofilen
 - Passwortvergabe/Passwortregeln
 - Personenkontrolle beim Empfang
 - Sorgfältige Auswahl von Reinigungspersonal
 - Verschlüsselung von Datenträgern
- Zugriffskontrolle:
 - Anzahl der Administratoren auf das Mindeste begrenzt
 - Einsatz von Aktenvernichtern
 - Erstellen eines Berechtigungskonzepts
 - Passwortrichtlinie inkl. Länge und Wechsel
 - Physische Löschung von Datenträgern vor deren Wiederverwendung
 - Sichere Aufbewahrung von Datenträgern
 - Verschlüsselung von Datenträgern
 - Verwaltung der Benutzerrechte durch Systemadministratoren

- Trennungskontrolle:

Erstellen eines Berechtigungskonzepts

Festlegung von Datenbankrechten

Logische Mandantentrennung (softwareseitig)

Trennung von Produktiv- und Testsystem

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO):

Eine Pseudonymisierung findet auf Anfrage statt

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

- Weitergabekontrolle:

Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen

Einrichtung von VPN-Tunneln

- Eingabekontrolle:

Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Protokollierung der Eingabe, Änderung und Löschung von Daten

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

- Verfügbarkeitskontrolle:

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Erstellen eines Backup & Recoverykonzepts /

Backup-Strategie (offline, online z.B. Cloud)

Feuer- und Rauchmeldeanlagen

Klimaanlagen in Serverräumen

Schutzsteckdosenleisten in Serverräumen

Testen von Datenwiederherstellung

Unterbrechungsfreie Stromversorgung (USV)

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

Backup Konzept (Offline / Online in der Cloud)

Nottfallmanagement Übungen (incl. worst-case)

Testen der Wiederherstellungssysteme

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

- Datenschutz-Management:

Externe Testierung / Prüfung

Interne Revision

Regelmäßige Datenschutz Audits

- Incident-Response-Management:

Alarmsysteme bei Dateneinbruch über das Internet (Firewall)

Monitoring von Datenzugriffen

Regelmäßige Datenschutzzschulungen, in denen die Mitarbeiter unterwiesen werden

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO):

Eigenentwicklungen

Manuelle Löschung auf Anforderung

Manuelle Löschung nach gesetzlicher Vorgabe

Manuelle Softwareunterstützung

- Auftragskontrolle:

Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28

DS-GVO

Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Vertragsstrafen bei Verstößen

Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender

Dokumentation

Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren