

Vereinbarung

über Auftragsverarbeitung gemäß Artikel 28 DSGVO

zwischen

XXX

XXX

XXX

- Verantwortlicher/Auftraggeber (AG) -

und

XXX

XXX

XXX

-Auftragsverarbeiter/Auftragnehmer (AN) -

§ 1 Umfang, Art und Zweck der Auftragsdatenverarbeitung

(1) Der AN erhebt, speichert, verändert, übermittelt, sperrt oder löscht Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person („personenbezogene Daten“) nur im Auftrag und nach Vorgabe des AG (Auftragsverarbeitung). Der AG erteilt alle Aufträge oder Teilaufträge in der Regel schriftlich. Mündliche Vorgaben sind vom AG unverzüglich schriftlich zu wiederholen.

(2) Der AN darf personenbezogene Daten ferner nur erheben, verarbeiten oder nutzen, soweit dies zur Erbringung der vereinbarten Leistungen erforderlich ist. Der AG bleibt für die Einhaltung der Vorschriften der DSGVO und anderer Vorschriften über den Datenschutz verantwortlich. Der AN garantiert, bei der Auftragsverarbeitungen sämtliche rechtlichen Bestimmungen einzuhalten.

(3) Ist der AN der Ansicht, dass eine Vorgabe des AG gegen die DSGVO oder andere Vorschriften über den Datenschutz verstößt, hat der AN den AG unverzüglich daraufhinzuweisen.

(4) Zweck der Auftragsdatenverarbeitung ist es, dass der AN auf die Daten zugreifen kann, die zur Erbringung der vereinbarten Leistungen erforderlich sind.. Die Datenverarbeitung findet ausschließlich innerhalb des Europäischen Wirtschaftsraums statt.

(5) Personenbezogene Daten werden vom AN ausschließlich für die Zwecke der vereinbarten Leistungen verarbeitet.

§ 2 Art der Daten und Kategorien betroffener Personen

(1) Der AN verarbeitet die Art der personenbezogenen Daten, welche in der Leistungsvereinbarung konkret beschrieben werden oder die Gegenstand der Verarbeitung personenbezogener Daten sind und folgenden Datenarten bzw. Datenkategorien entsprechen:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail-Adresse)
- Sammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Abrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(2) Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben oder betreffen bzw. umfassen folgende Personen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner

(3) Besondere Arten personenbezogener Daten (Art. 9 DSGVO) sind:

- Gesundheit/Sexualleben
- Gewerkschaftszugehörigkeit/Betriebsrat
- Religiöse/weltanschauliche Überzeugungen
- Politische Meinungen
- Rassistische/ethnische Herkunft
- Genetische/biometrische Daten
- Gesichtsbilder zur eindeutigen Identifizierung

§ 3 Technische und organisatorische Maßnahmen

(1) Der AN 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 AG zur Prüfung zu übergeben. Bei Akzeptanz durch den AG werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des AG einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der AN hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen.

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

§ 4 Berichtigung, Einschränkung und Löschung von Daten

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

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

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

(2) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt und dessen Kontaktdaten dem AG zum Zweck der direkten Kontaktaufnahme mitgeteilt werden.

(3) Als Datenschutzbeauftragter bestellt der AN folgende Person:

Herr/Frau:

Organisationseinheit:

Telefon:

E-Mail

dessen jeweils aktuelle Kontaktdaten auf der WebSite des AN leicht zugänglich hinterlegt sind. In Wechsel des Datenschutzbeauftragten ist dem AG unverzüglich mitzuteilen.

(4) Der Auftragnehmer ist zur Bestellung eines Datenschutzbeauftragten nicht verpflichtet. Ansprechpartner ist der genannte Auftragnehmer.

(5) Zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO setzt der AN nur Beschäftigte bzw. beauftragte Dritte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden sowie die Daten ausschließlich entsprechend der Vorgabe des AG verarbeiten.

§ 6 Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.

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

(2) Soweit der AG 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 AN ausgesetzt ist, hat ihn der AN nach besten Kräften zu unterstützen.

(3) Der AN 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. Hierzu gehört auch die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem AG im Rahmen seiner Kontrollbefugnisse.

§ 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 AN 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 AN ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Sofern der AN weitere Unterauftragnehmer als Auftragsdatenverarbeiter beauftragt, hat er eine derartige Beauftragung dem AG unverzüglich anzuzeigen.

(3) Die Weitergabe von personenbezogenen Daten 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 AN die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Der AN hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem AG auf Verlangen unverzüglich vorzulegen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der AG hat das Recht, im Benehmen mit dem AN 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 AN in dessen Geschäftsbetrieb zu überzeugen. Der AG erteilt alle Aufträge, Teilaufträge oder Vorgaben schriftlich oder in Textform. In Eilfällen können Vorgaben mündlich erteilt werden; diese wird der AG unverzüglich schriftlich oder in Textform bestätigen.

(2) Der AN stellt sicher, dass sich der AG von der Einhaltung der Pflichten des AN nach Art. 28 DSGVO überzeugen kann. Der AN verpflichtet sich, dem AG 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 durch die Bereitstellung aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) erfolgen.

§ 9 Mitteilung bei Verstößen des Auftragnehmers

(1) Der AN unterstützt den AG bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

(2) Zu den in Absatz 1 genannten Maßnahmen 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 Verletzungsereignissenermöglich
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den AG zu melden
- die Verpflichtung, dem AG 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 AG für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des AG im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

§ 10 Befugnisse des Auftraggebers

(1) Mündliche Vorgaben bestätigt der AG unverzüglich mindestens in Textform.

(2) Der AN hat den AG unverzüglich zu informieren, wenn er der Meinung ist, eine Vorgabe verstoße gegen Datenschutzvorschriften. Der AN ist berechtigt, die Durchführung der entsprechenden Vorgabe so lange auszusetzen, bis sie durch den AG bestätigt oder geändert wird.

§ 11 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten dürfen ohne Wissen des AG nicht erstellt werden. 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 Erbringung der vereinbarten Leistungen oder früher nach Aufforderung durch den AG – spätestens mit Beendigung der Leistungsvereinbarung – hat der AN sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG 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 AN entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung nach Erbringung der Leistung dem AG übergeben.

XXX, den XX.XX.XXXX

XXX, den XX.XX.XXXX

Unterschrift AG

Unterschrift AN