

Vertrag zur Auftragsverarbeitung

zwischen

- Auftragsverarbeiter - nachstehend „Auftragnehmer“ genannt

und der

windata GmbH & Co. KG, Gegenbaurstr. 4, 88239 Wangen -

Verantwortlicher - nachstehend „Auftraggeber“ genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Dienstleistungsvertrag/ Rahmenvertrag vom _____, auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

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

(Definition der Aufgaben)

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum

oder

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

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorhergesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom

oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

(2) Ort der Datenverarbeitung

2.1 Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

2.2. Die Übermittlung personenbezogener Daten in ein Drittland oder an internationale Organisationen bedarf der vorherigen Zustimmung des Auftraggebers. Sie wird nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 50 DSGVO erfüllt sind.

2.3 Erfolgt die Übermittlung auf Grundlage von EU-Standardvertragsklauseln, so sichert der Auftragnehmer zu, dass er diese einhalten kann und nicht durch gesetzliche oder andere rechtliche Anforderungen daran gehindert ist. Der Auftragnehmer gibt auf Anfrage Auskunft über die in seinem Land geltenden Gesetze (insbesondere Zugriffsmöglichkeiten durch Behörden des Drittlandes auf die Daten, den Parteien und den betroffenen Personen zustehende Rechtsschutzmöglichkeiten, Rechtsprechung und Behördenpraxis im Drittland mit Bezug zum Datenschutzniveau und zum Rechtssystem insgesamt) und weist nach, dass sie den durch die EU-Standardvertragsklauseln gewährten Schutz nicht untergraben.

2.4 Sofern der Schutz der im Auftrag verarbeiteten personenbezogenen Daten durch Gesetze oder eine sonstige Praxis im Zielland beeinträchtigt wird, hat der Auftragnehmer zusätzliche Maßnahmen (z. B. Verschlüsselung, Anonymisierung, Pseudonymisierung, Trustee-Lösung etc.) umzusetzen, um einen wirksamen Schutz herzustellen. Der Auftragnehmer gibt auf Anfrage Auskunft über die ergriffenen zusätzlichen Maßnahmen.

2.5 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er nicht mehr in der Lage ist, die EU-Standardvertragsklauseln einzuhalten; in diesem Fall darf der Auftraggeber die Datenübermittlung aussetzen und den Hauptvertrag mit dem Auftragnehmer kündigen. Der Auftragnehmer hat betroffene Personen verschuldensunabhängig von allen Schäden freizustellen, die durch den Zugriff von Stellen seines Staates bzw. am Ort der Datenverarbeitung außerhalb der EU auf die Daten der betroffenen Personen entstehen.

(3) Art der Daten

Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:

oder

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

Personendatenstamm

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

Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Kundenhistorie

Vertragsabrechnungs- und Zahlungsdaten

Planungs- und Steuerungsdaten

Auskunftsangaben (von Dritten, z.B. Auskunftsteien, oder aus öffentlichen Verzeichnissen)

Sonstige:

(4) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:

oder

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Kunden

Interessenten

Abonnenten

Beschäftigte

Zahlungspflichtige/Zahlungsempfänger

Ansprechpartner

Sonstige:

3. 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 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 Auftragnehmer 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 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 nicht vom Leistungsumfang umfasst, sind Löschkonzepte, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer 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:

Schriftliche Bestellung eines Datenschutzbeauftragten/einer Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Dessen/Deren Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des/der Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Als externer Datenschutzbeauftragter ist beim Auftragnehmer PRW Consulting GmbH, Leonrodstrasse 54, 80636 München, Herr Marcel Erntges, Tel.: +49 (0)89 / 2109 77 - 70, E-Mail: marcel.erntges@prw-consulting.de bestellt. Stellvertreterin ist windata GmbH & Co. KG, Gegenbaurstr. 4, 88239 Wangen, Tel.: +49 (0) 7522 / 9770-0, E-Mail: datenschutz@windata.de. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Dessen/Deren jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner_in beim Auftragnehmer wird

Anrede

Name, Vorname

Organisationseinheit

Telefon

E-Mail

benannt.

Der Auftragnehmer hat seinen Sitz außerhalb der Union und benennt folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union

Land

Anrede

Name, Vorname

Organisationseinheit

Telefon

E-Mail

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) 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 berechtigterweise 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.
- b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- c) 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.
- d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationensuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seine Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrags.
- g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
- h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.
- i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz Aufsichtsbehörde.

6. 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.

Eine Unterbeauftragung ist unzulässig

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma

Anschrift

Leistung

Unterauftragnehmer

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 Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen einmaliges 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;

bedarf einer ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. 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 DSGVO 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 DSGVO;

die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

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-Grundschrift).

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

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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 relevanten Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
- 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 angemessene Vergütung beanspruchen.

9. 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.

10. Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien und Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsmäßigen 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 ordnungsmäßigen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zur Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort und Datum

Ort und Datum

Unterschrift(en) Auftraggeber

Unterschrift(en) Auftragnehmer

Bitte fügen Sie als Auftragnehmer, Ihre „allgemeine Datenschutzerklärung“ und die „technischen und organisatorischen Maßnahmen“ gemäß DSGVO bei.

Diese sollten folgende Maßnahmen enthalten:

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungskontrolle