

Vertrag zur Auftragsverarbeitung gemäß Artikel 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Vertrag

zwischen dem „Verantwortlichen“ (im Sinne des Art. 4 Nr. 7 DSGVO)

Stadt Rheine
vertreten durch den Bürgermeister
Fachbereich/Sonderbereich/Produkt
Klosterstraße 14
48431 Rheine

(im Folgenden Auftraggeber genannt)

und dem „Auftragsverarbeiter“ (im Sinne des Art. 4 Nr. 8 DSGVO)

Firmenname
gesetzl. Vertretung
Adresse

(im Folgenden Auftragnehmer genannt)

Präambel

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zur Sicherstellung der Durchführung der gesetzlichen Vorschriften bei der Verarbeitung personenbezogener Daten im Auftrag und regelt abschließend den Datenschutz zwischen den Vertragsparteien.

1. Gegenstand, Dauer und Spezifizierung des Vertrags

a) Gegenstand des Vertrags

Im Rahmen des Vertragsgegenstandes verarbeitet der Auftragnehmer personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

Der Gegenstand des Auftrags umfasst eine [z. B. das Hosting, die Administration, die Wartung, den Betrieb des Fachverfahrens ...] Näheres ergibt sich aus der Leistungsvereinbarung/dem Vertrag [Bezeichnung] mit der Vertragsnummer [Nummer], auf die hier verwiesen wird.

Der Auftragnehmer unterwirft sich bezüglich der Verarbeitung von personenbezogenen Daten denselben Anforderungen, die für den Auftraggeber gelten, insbesondere dem jeweiligen Datenschutzgesetz des Bundeslandes, welches für den Auftraggeber

wirksam ist. Dabei beachtet der Auftragnehmer insbesondere die einschlägigen Vorschriften der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes sowie des Datenschutzgesetzes Nordrhein-Westfalen in der jeweils gültigen Fassung der Bekanntmachung.

b) **Dauer des Vertrags**

Der Vertrag beginnt am **DATUM** und wird auf unbestimmte Zeit geschlossen. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer die Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten Pflichten stellt einen schweren Verstoß dar.

2. Konkretisierung des Auftragsinhalts

a) **Art und Zweck der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO)**

Die Dienstleistungen des Auftragnehmers umfassen

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verfahrensregeln).

b) **Art der Daten**

Art der verwendeten personenbezogenen Daten sind

- **Stammdaten**
- **Kommunikationsdaten**
- **Finanzdaten**
- **etc.**

c) **Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen

- **Beschäftigte**
- **Bürger/-innen**
- **etc.**

3. Rechte und Pflichten des Auftraggebers

a) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer

verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

- b) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- c) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- d) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
- e) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- f) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrags bestehen.

4. Pflichten des Auftragnehmers

- a) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, ausschließlich im Rahmen des abgeschlossenen Vertrags und nach Weisung des Auftraggebers verarbeiten. Sofern der Auftragnehmer durch nationales oder europäisches Recht zu einer hiervon abweichenden Verarbeitung verpflichtet ist, weist er – sofern dies rechtlich zulässig ist – den Auftraggeber vor Beginn der Verarbeitung auf diesen Umstand hin (§ 28 Abs. 3 lit. a DSGVO). Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
- b) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen 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 (Art. 28 Abs. 3 Satz lit. b, Art 29 DSGVO) oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Vertrags fort.
- c) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgenabschätzungen des Auftrag-

gebers hat der Auftragnehmer in notwendigem Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO) sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

- d) Der Auftragnehmer kontrolliert 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 Personen gewährleistet wird. Das Ergebnis der Kontrollen ist zu dokumentieren und auf Anfrage dem Auftraggeber zur Verfügung zu stellen.
- e) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarung im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 lit. h DSGVO).
- f) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 lit. f DSGVO). Meldungen nach Art. 33 und 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.
- g) Der Auftragnehmer hat schriftlich eine/n Datenschutzbeauftragte/n benannt, die/der die Tätigkeit gem. Art. 38 und 39 DSGVO ausübt. **Sie/er ist unter folgenden Kontaktdaten zu erreichen:**
- h) Auftragnehmer und Auftraggeber arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer 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. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Unterauftragsverhältnisse mit Subunternehmen (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

- a) 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 Auftraggeber 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.
- b) Der Einsatz von Subunternehmen als weitere Auftragsverarbeiter ist nur mit vorheriger Zustimmung des Auftraggebers gestattet (Art. 28 Abs. 2 DSGVO). Die Genehmigung ist schriftlich (mindestens per E-Mail) einzuholen.
- c) Eine Beauftragung von Unterauftragsnehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- d) Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).
- e) Eine Weiterleitung der Daten an den Unterauftragnehmer ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt.
- f) 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.

- g) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragsunternehmen zu:

Firma/Unterauftragsnehmer

Anschrift/Land

Leistung

7. Technisch-organisatorische Maßnahmen

- a) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe vereinbarten erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. **Die umzusetzen- den technischen und organisatorischen Maßnahmen sind am Ende dieses Vertrags dargestellt (Anlage).** Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und zu dokumentieren.
- b) 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.

- c) 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. Darüber hinaus beobachtet der Auftragnehmer die technische Entwicklung und schlägt ggf. notwendige Anpassungen der technisch-organisatorischen Maßnahmen vor.

8. Verpflichtung des Auftragnehmers während und nach Beendigung des Auftrags, Art. 28 Abs. 3 S. 2 lit. g DSGVO

- a) 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 gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, 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.
- b) 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.

9. Haftung

- a) Der Auftragnehmer haftet für Schäden, die der Auftraggeber, seine Beschäftigten bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder sein Unterauftragnehmer bei der Erbringung der vertraglichen Leistung verursachen.
- b) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadenersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten (Art. 82 DSGVO).
- c) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

10. Sonstiges

- a) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ergebnisse 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 „Verantwortlichem“ im Sinne der DSGVO liegen.
- b) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich des Anspruches auf Rückgabe der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- c) Gerichtsstand ist, wenn im Dienstleistungsvertrag nichts anderes vereinbart ist, Rheine.

11. Wirksamkeit des Vertrags

Dieser Vertrag bleibt auch bei rechtlicher Unwirksamkeit einzelner Punkte in seinen übrigen Teilen verbindlich. Unwirksame Bestimmungen sind von den Parteien durch wirksame zu ersetzen, die dem gewollten Zweck möglichst nahekommen. Entsprechendes gilt im Falle einer Vertragslücke.

Ort, Datum

Ort, Datum

Auftragnehmer

Auftraggeber

Ggf. sind als Anlage die technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO vom Auftragnehmer zu ergänzen (siehe Punkt 7 a dieses Vertrags).