

# Auftragsverarbeitungsvertrag (AVV)

nach Art-. 28 Datenschutzgrundverordnung (DSGVO)

zwischen

Musterfirma  
Musterstraße 123  
12535 Musterstadt

- nachfolgend „**Auftraggeber**“ genannt -

und

Donau Data Engineering GmbH  
Marie-Curie-Straße 1  
26129 Oldenburg

- nachfolgend „**Auftragnehmer**“ genannt -

**zum Zwecke der Nutzung des TASKO® Softwaresystems**  
(Cloudlösung zur Prozessdatenerfassung und -dokumentation)

## Präambel

Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Rahmen einer Auftragsverarbeitung im Sinne von Art. 28 DSGVO im Zusammenhang mit der Bereitstellung und Nutzung des cloudbasierten TASKO®-Systems durch den Auftraggeber.

Das TASKO®-System dient der strukturierten Erfassung, Auswertung und Dokumentation von Prozessdaten, die je nach Anwendungsfall personenbezogene Daten enthalten können. Der Auftragnehmer verarbeitet diese Daten ausschließlich auf Weisung des Auftraggebers und in dessen Verantwortung. Die Parteien verpflichten sich zur Einhaltung sämtlicher anwendbarer Datenschutzvorschriften, insbesondere der DSGVO.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Anforderungen der Zusammenarbeit zwischen Auftraggeber und Auftragnehmer und bildet die Grundlage für einen verantwortungsvollen und sicheren Umgang mit personenbezogenen Daten.

## 1. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

## 2. Dauer des Auftrags

(1) Dieser Vertrag tritt mit Unterzeichnung durch beide Parteien in Kraft und gilt für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers. Mit Beendigung des Hauptvertrages endet auch dieser Vertrag automatisch. Die Verpflichtungen hinsichtlich Rückgabe oder Löschung personenbezogener Daten sind in **Punkt 15** festgelegt.

(2) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

## 3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Ergänzende Weisungen des Auftraggebers, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, gelten als Zusatzleistungen. Der dadurch entstehende Mehraufwand ist vom Auftraggeber nach Aufwand zu vergüten, und zwar zu einem Stundensatz von 128,50€ netto oder nach anderer Vereinbarung.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 4** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich

#### **4. Pflichten des Auftragnehmers**

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der vom Auftraggeber erteilten, ergänzenden, dokumentierten Weisungen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer gegebenenfalls zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall informiert der Auftragnehmer den Auftraggeber über die rechtlichen Anforderungen und die beabsichtigte Verarbeitung, sofern das geltende Recht keine Mitteilung wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer wird die Datenverarbeitung (Hosting) **ausschließlich in der Bundesrepublik Deutschland** durchführen. Dem Auftragnehmer ist eine Datenverarbeitung außerhalb von Deutschland nur für Zwecke des technischen Supports und der Kommunikation (z. B. via Microsoft Teams oder Zoom) erlaubt. Details zur Infrastruktur und Zertifizierung sind der **Anlage 2.1** zu entnehmen.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 5 Werktagen, darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann (z. B. aufgrund einer unzulässigen Verarbeitung oder Verletzung der Rechte der betroffenen Personen), steht dem Auftragnehmer das Recht zu, die weitere Verarbeitung auszusetzen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung für einen Zeitraum von maximal 10 Werktagen auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(4) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner Pflichten gem. Art. 32–36 DSGVO. Die Art und Weise der Unterstützung ergibt sich aus **Anlage 1**, die Bestandteil dieses Vertrags ist.

## 5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt zu haben und stellt sicher, dass dieser über die erforderliche Qualifikation und Fachkunde verfügt. Name und Kontaktdaten sind in **Anlage 1** dokumentiert.

(2) Eine Benennung kann entfallen, sofern der Auftragnehmer nachweist, dass keine gesetzliche Verpflichtung besteht und interne Regelungen die datenschutzkonforme Verarbeitung gemäß Gesetz, Vertrag und Weisungen des Auftraggebers sicherstellen.

## 6. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der Auftragnehmer sichert zu, dass er die im Zeitpunkt des Vertragsschlusses vereinbarten technischen und organisatorischen Maßnahmen (TOM) im Sinne von Art. 32 DSGVO, wie sie in der **Anlage 2 sowie der ergänzenden Zusatzerklärung zum Hosting (Anlage 2.1)** zu diesem Vertrag niedergelegt sind, umsetzt und während der Vertragslaufzeit aufrechterhält. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

## 7. Rechte Betroffener und Mitwirkungspflichten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den

Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Sofern dem Auftragnehmer im Zusammenhang mit der Geltendmachung von Betroffenenrechten gemäß Art. 15 ff. DSGVO durch betroffene Personen gegenüber dem Auftraggeber Mitwirkungspflichten entstehen, ist der hierdurch entstehende Mehraufwand vom Auftraggeber gesondert zu vergüten. Die Vergütung erfolgt nach Vereinbarung. Der Auftragnehmer weist den Aufwand durch geeignete Tätigkeitsnachweise nach. Keine Vergütung erfolgt, sofern die Mitwirkung aufgrund eines gesetzes- oder vertragswidrigen Verhaltens des Auftragnehmers erforderlich wurde.

## **8. Meldepflichten des Auftragnehmers**

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

## 9. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, Unterauftragnehmer (Subunternehmer) mit der Erbringung von Leistungen im Rahmen dieses Vertrags zu beauftragen, sofern mit diesen ein Auftragsverarbeitungsvertrag abgeschlossen wird, der den Anforderungen von Art. 28 DSGVO genügt.

(2) Der Auftragnehmer verpflichtet sich, diesen Unterauftragnehmern mindestens gleichwertige Datenschutzpflichtenaufzuerlegen, wie sie sich aus diesem Vertrag ergeben. Insbesondere gewährleistet der Auftragnehmer, dass diese Unterauftragnehmer hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen im Sinne des Art. 28 Abs. 1 DSGVO bieten.

(3) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen an der in **Anlage 3** aufgeführten Liste von Unterauftragnehmern. Der Auftraggeber kann diesen Änderungen innerhalb von 14 Kalendertagen aus wichtigem Grund schriftlich widersprechen. Erfolgt kein Widerspruch innerhalb dieser Frist, gelten die Änderungen als genehmigt. Auf Anfrage stellt der Auftragnehmer dem Auftraggeber aussagekräftige Auszüge der relevanten datenschutzbezogenen Vertragsbestandteile mit dem jeweiligen Unterauftragnehmer zur Verfügung, soweit dies zur Wahrung der Rechenschaftspflicht erforderlich ist. Die Offenlegung unterliegt dem Vorbehalt der Wahrung von Geschäftsgeheimnissen und Sicherheitsinteressen.

(4) Nicht als Unterauftragsverhältnisse i.S.d. Absatz 1 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste.

(5) Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

## **10. Kontrollrechte**

(1) Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen Datenschutzvorschriften (insbesondere der DSGVO), der in diesem Vertrag festgelegten Pflichten sowie seiner erteilten Weisungen durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

Die Kontrolle kann insbesondere erfolgen durch:

- Einsichtnahme in Dokumentationen, Zertifikate, Prüfberichte oder Auditprotokolle
- Anforderung von schriftlichen Auskünften
- Vor-Ort-Kontrollen nach rechtzeitiger Ankündigung (i.d.R. 14 Kalendertage im Voraus),
- Durchführung von Fern-Audits mittels Videokonferenz oder Remote-Zugriff

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber bei der Durchführung der in (9.1) genannten Kontrollen aktiv zu unterstützen und ihm alle erforderlichen Informationen und Nachweise zur Verfügung zu stellen, die zur Prüfung der Einhaltung der datenschutzrechtlichen Vorgaben erforderlich sind. Der Auftragnehmer ermöglicht die Einsicht in relevante Dokumente und beantwortet Rückfragen innerhalb angemessener Frist.

(3) Vor-Ort-Kontrollen erfolgen nur nach rechtzeitiger Anmeldung und unter Berücksichtigung betrieblicher Abläufe. Die Parteien stimmen sich über Umfang, Ort und Zeit der Kontrolle vorher ab. Der Auftraggeber verpflichtet sich, die Kontrolle nur im erforderlichen Umfang durchzuführen und den Betriebsablauf des Auftragnehmers möglichst nicht unverhältnismäßig zu beeinträchtigen. Sollte die Kontrolle in sicherheitssensiblen Bereichen (z. B. Rechenzentren) nicht möglich sein, kann der Auftragnehmer auf alternative Nachweismittel (z. B. Testate, Zertifikate) verweisen.

(4) Der Auftragnehmer kann für Vor-Ort-Kontrollen angemessene Aufwände (insbesondere Personalkosten für die Begleitung der Kontrolle) geltend machen. Der dadurch entstehende Mehraufwand ist vom Auftraggeber nach Aufwand zu vergüten, und zwar zu einem Stundensatz von 128,50€ netto oder nach anderer Vereinbarung.

## **11. Vertraulichkeitsverpflichtung**

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

## **12. Geheimhaltungspflichten**

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

## **13. Datenverarbeitung im Home-Office**

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office“ verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office“ durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte im „Home-Office“ eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.



## 14. Ort der Datenverarbeitung und Hosting

(1) **Exklusiver Hosting-Standort:** Die Speicherung und Verarbeitung der personenbezogenen Daten erfolgt ausschließlich in zertifizierten Rechenzentren innerhalb der **Bundesrepublik Deutschland**. Ein physisches Hosting der Daten in anderen Mitgliedstaaten der EU, des EWR oder in Drittländern ist ausgeschlossen.

(2) **Drittlandsbezug und Support:** Eine Übermittlung von Daten in ein Drittland (z. B. im Rahmen von Wartung oder technischem Support durch Subunternehmer) ist grundsätzlich **nicht vorgesehen**. Sollte eine solche Übermittlung im Ausnahmefall zwingend erforderlich sein, darf sie nur erfolgen, wenn:

- der Auftraggeber vorab **schriftlich zugestimmt** hat,
- die strengen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss oder Standardvertragsklauseln) und
- ein dem Schutzniveau der DSGVO entsprechendes Datenschutzniveau beim Empfänger garantiert ist.

(3) **Sicherstellung bei Unterauftragnehmern:** Der Auftragnehmer stellt durch vertragliche Vereinbarungen und regelmäßige Kontrollen sicher, dass auch etwaige Unterauftragnehmer die Anforderungen dieses Paragraphen sowie die strengen Vorgaben zum Hosting-Standort Deutschland vollumfänglich einhalten.

## 15. Rückgabe und Löschung von Daten bei Vertragsende

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinem Besitz befindlichen personenbezogenen Daten, Unterlagen und Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit diesem Vertrag stehen, nach Wahl des Auftraggebers entweder an diesen zurückzugeben oder datenschutzkonform zu löschen. Die Durchführung der Löschung ist in geeigneter Weise zu dokumentieren.

Dies gilt nicht, soweit gesetzliche Aufbewahrungspflichten entgegenstehen oder eine Speicherung zur Wahrung berechtigter Interessen des Auftragnehmers erforderlich ist. In diesen Fällen erfolgt eine Sperrung der Daten.

Die Rückgabe oder Löschung erfolgt innerhalb von 30 Kalendertagen nach Vertragsende. Die Rückgabe erfolgt in einem branchenüblichen, strukturierten, maschinenlesbaren Format. Erheblicher Mehraufwand für ein vom Standard abweichendes Format kann gesondert vergütet werden.

(2) Der Auftragnehmer haftet im Zusammenhang mit der Rückgabe oder Löschung personenbezogener Daten nach Vertragsende ausschließlich bei schuldhafter Verletzung seiner vertraglichen oder gesetzlichen Pflichten. Eine Haftung besteht insbesondere nicht, wenn eine Löschung oder Rückgabe aufgrund gesetzlicher

Aufbewahrungspflichten unterbleibt, die dem Auftragnehmer obliegen, oder wenn der Auftraggeber die erforderlichen Weisungen zur Rückgabe oder Löschung nicht rechtzeitig, nicht eindeutig oder nicht vollständig erteilt hat. Die Beweislast für das Vorliegen eines schuldhaften Verhaltens des Auftragnehmers liegt beim Auftraggeber. Die gesetzlichen Regelungen zur gemeinsamen Haftung nach Art. 82 DSGVO bleiben hiervon unberührt.

## **16. Vergütung**

Eine etwaige Vergütung für Leistungen ist, sofern nicht ausdrücklich im Vertrag geregelt, gesondert zwischen den Parteien zu vereinbaren.

## **17. Haftung und Schadensersatz**

(1) Beide Parteien haften einander nach Maßgabe der gesetzlichen Bestimmungen für Schäden, die aus einer schuldhaften Verletzung der in diesem Vertrag oder der DSGVO geregelten Pflichten entstehen.

(2) Der Auftragnehmer haftet ausschließlich, wenn und soweit ihm ein Verstoß gegen datenschutzrechtliche Vorschriften nachgewiesen werden kann, insbesondere gemäß Art. 82 Abs. 3 DSGVO.

Die Haftung des Auftragnehmers ist auf Schäden beschränkt, die auf vorsätzliche oder grob fahrlässige Pflichtverletzungen zurückzuführen sind. Für einfache Fahrlässigkeit haftet der Auftragnehmer nur bei der Verletzung wesentlicher Vertragspflichten (Kardinalpflichten), jedoch der Höhe nach auf den typischerweise vorhersehbaren Schaden begrenzt.

(3) Soweit der Auftraggeber für Verstöße haftet, die auf unzutreffende Weisungen oder Pflichtverletzungen des Auftraggebers zurückzuführen sind, ist der Auftragnehmer von einer daraus resultierenden Inanspruchnahme Dritter freizustellen.

(4) Die Parteien verpflichten sich, sich im Innenverhältnis anteilig im Verhältnis zur jeweiligen Verantwortlichkeit gemäß Art. 82 Abs. 5 DSGVO zu beteiligen, sofern eine gemeinsame Haftung gegenüber betroffenen Personen oder Aufsichtsbehörden festgestellt wird.

## **18. Zurückbehaltungsrecht**

(1) Der Auftragnehmer verzichtet im Grundsatz auf die Geltendmachung eines Zurückbehaltungsrechts gemäß § 273 BGB an personenbezogenen Daten oder zugehörigen Datenträgern, soweit dies zur Erfüllung der gesetzlichen oder vertraglichen Pflichten des Auftraggebers erforderlich ist. Die Herausgabe, Löschung oder Sperrung der verarbeiteten personenbezogenen Daten bleibt auch bei bestehenden Meinungsverschiedenheiten oder Zahlungsrückständen möglich und erfolgt auf Grundlage der vertraglichen Vereinbarungen.

(2) Davon unberührt bleibt das Recht des Auftragnehmers, im Falle von erheblichen Pflichtverletzungen des Auftraggebers – insbesondere bei mehrmaligem Zahlungsverzug trotz Mahnung – die Erbringung nicht unmittelbar datenschutzrelevanter Zusatzleistungen (z. B. Support, Dokumentation, Zusatzfunktionen) bis zur Klärung der Angelegenheit vorübergehend einzuschränken oder auszusetzen. Die datenschutzrechtlichen Kernpflichten des Auftragnehmers gemäß diesem Vertrag bleiben hiervon unberührt.

## **19. Schlussbestimmung**

### **(1) Gefährdung der Daten durch Dritte**

Sollten personenbezogene Daten oder andere vertraglich geschützte Informationen des Auftraggebers, die sich im Besitz oder unter der Kontrolle des Auftragnehmers befinden, durch Maßnahmen Dritter (z. B. Pfändung, Beschlagnahme, Insolvenzverfahren) oder durch sonstige Ereignisse gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich. Der Auftragnehmer wird in diesen Fällen die betreffenden Dritten unverzüglich darüber informieren, dass es sich um Daten handelt, die ausschließlich im Auftrag und auf Weisung des Auftraggebers verarbeitet werden und dem besonderen Schutz nach Art. 28 DSGVO unterliegen.

### **(2) Nebenabreden und Schriftform**

Änderungen und Ergänzungen dieses Vertrags sowie Nebenabreden bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis.

### **(3) Salvatorische Klausel**

Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Anstelle der unwirksamen oder undurchführbaren Bestimmung gilt eine Regelung als vereinbart, die dem wirtschaftlichen Zweck der ursprünglichen Regelung in rechtswirksamer Weise am nächsten kommt. Gleiches gilt im Falle einer Regelungslücke.

\_\_\_\_\_  
Ort/Datum

Oldenburg, den 9. Februar 2026



\_\_\_\_\_  
- Auftraggeber -

\_\_\_\_\_  
- Auftragnehmer -