Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO (Datenschutz-Grundverordnung)

zwischen

Kunde/Handwerker
- Verantwortlicher -

und

One4Business Solutions GmbH
- Auftragsverarbeiter -

§ 1 Vertragsgegenstand

(1) Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten" genannt) durch den Auftragsverarbeiter für den Verantwortlichen in dessen Auftrag und nach dessen Weisung.

Die Beauftragung durch den Verantwortlichen wird durch die AGB Sonepar Hero bestimmt (nachstehend Hauptvertrag genannt).

Die konkreten Verarbeitungstätigkeiten der Auftragsverarbeitung im Zusammenhang mit dem Hauptvertrag, insbesondere die Art der Daten, der Zweck der Datenerhebung, Datenverarbeitung und -nutzung, sowie der Kreis der Betroffenen sind in **AVV-Anlage 1** festgelegt.

Jede von den Festlegungen in **AVV-Anlage 1** abweichende oder darüberhinausgehende Verarbeitung von Daten ist dem Auftragsverarbeiter untersagt, insbesondere eine Verarbeitung der Daten des Verantwortlichen zu eigenen Zwecken.

§ 2 Verantwortlichkeit

(1) Der Verantwortliche ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen als Verantwortlicher der Verarbeitung im Sinne des Art. 4 Nr. 7 DSGVO allein verantwortlich. Dieses gilt insbesondere für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der Betroffenen nach den Art. 12 bis 22 DSGVO.

(2) Die Inhalte dieses AV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen (IT-Systemen) im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Der Auftragsverarbeiter ist für die Einhaltung der jeweils für ihn als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO einschlägigen Datenschutzvorschriften, insbesondere des Art. 28 DSGVO, verantwortlich.

(4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 3 Weisungsbefugnis des Verantwortlichen

(1) Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragsverarbeiter eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragsverarbeiter unterrichtet soweit möglich in derartigen Situationen den Verantwortlichen vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Die Weisungen sind vom Auftragsverarbeiter, sowie vom Verantwortlichen in schriftlicher Form oder in Textform zu dokumentieren.

(2) In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen bestätigt der Verantwortliche im Nachgang unverzüglich (mind. Textform). Die weisungsberechtigten Personen sind in **AVV-Anlage 2** aufgeführt.

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

§ 4 Pflichten der Auftragsverarbeiter

(1) Der Auftragsverarbeiter verpflichtet, sich personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – zu verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der zuständigen Aufsichtsbehörde.

Hierzu gehören

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. Diese Maßnahmen muss der Auftragsverarbeiter auf Anfrage dem Verantwortlichen und ggfs. den Aufsichtsbehörden gegenüber nachweisen;

b) die Verpflichtung, Verstöße vom Auftragsverarbeiter oder der bei ihm im Rahmen des Auftrags beschäftigten Personen oder weiterer vom Auftragsverarbeiter beauftragter Auftragsverarbeiter gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder der im Vertrag getroffenen Festlegungen, unverzüglich an den Verantwortlichen zu melden. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Verantwortlichen ab. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Artt. 33, 34 DSGVO;

c) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung, mit allen ihm zur Verfügung stehenden Informationen;
d) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen der Aufsichtsbehörde.

(3) Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten des Verantwortlichen befassten Mitarbeitern und anderen für den Auftragsverarbeiter tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragsverarbeiter, dass sich die zur Verarbeitung der personenbezogenen Daten Befugten zur Vertraulichkeit und falls erforderlich auf das Fernmeldegeheimnis (§ 88 TKG) verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Hauptvertrages fort.

(4) Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person zu unterstützen, ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen und Anfragen von Betroffenen unverzüglich an den Verantwortlichen weiterzuleiten.

(5) Der Auftragsverarbeiter selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 2 DSGVO. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung. Auf Anfrage des Verantwortlichen stellt der Auftragsverarbeiter dem Verantwortlichen alle Angaben zur Verfügung, die zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DSGVO benötigt werden.

(6) Der Auftragsverarbeiter verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine wesentlichen Mittel zur Verarbeitung ein, die nicht vom Verantwortlichen zuvor genehmigt wurden. Legt der Auftragsverarbeiter unter Verstoß gegen die DSGVO Zwecke und Mittel selbst fest, gilt er in Bezug auf die Verarbeitung als Verantwortlichen.

(7) Eine Verarbeitung außerhalb der Räumlichkeiten vom Auftragsverarbeiter (z.B. im Homeoffice) ist zulässig. Der Auftragsverarbeiter hat dafür zu sorgen, dass auch in diesem Arbeitsumfeld angemessene technische und organisatorische Maßnahmen für die jeweilige Verarbeitungssituation mit ergriffen und deren Einhaltung in angemessener Form mit den betroffenen Beschäftigten des Auftragsverarbeiters vereinbart werden. Für die Beurteilung der Sicherheit der Verarbeitung stellt der Auftragsverarbeiter dem Verantwortlichen vorab auf Anforderung alle Informationen, insbesondere einen detaillierten Nachweis zur IT-Sicherheit und Richtlinien zur Arbeit im Homeoffice (z.B. Dienstanweisungen oder Betriebsvereinbarungen) zur Verfügung.

(8) Sollten die personenbezogenen Daten des Verantwortlichen bei dem Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Verantwortlichen als Verantwortlichem im Sinne der DSGVO liegen.

(9) Der Auftragsverarbeiter verpflichtet sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Verantwortlichen vertraulich zu behandeln.

(10) Die Erfüllung der vorgenannten Pflichten ist vom Auftragsverarbeiter zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Verantwortlichen auf Anforderung nachzuweisen.

§ 5 Technische und organisatorische Maßnahmen

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

(2) Der Auftragsverarbeiter 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 Festlegung des Schutzniveaus obliegt dem Verantwortlichen und wird anhand der Kriterien in **AVV-Anlage 3** festgelegt.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind dem Verantwortlichen rechtzeitig vorab in einer zur Überprüfung geeigneten Form mitzuteilen und zu dokumentieren.

§ 6 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zur Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet sie insbesondere die Einhaltung folgender Vorgaben:

a) Die Angaben hinsichtlich der Benennung eines Datenschutzbeauftragen (sofern erforderlich) oder eines Ansprechpartners für Fragen zum Datenschutz, siehe **AVV-Anlage 2**.

b) Der Verantwortlichen und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

d) Soweit der Verantwortlichen 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

e) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach § 9 dieses Vertrages.

f) Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

§ 7 Unterauftragsverhältnisse

(1) Unterauftragsverarbeiter im Sinne dieses Vertrags ist nur wer Leistungen erbringt, die direkt auf die Erbringung der Hauptleistung bezogen sind und die im Kernbereich auf eine Verarbeitung von personenbezogenen Daten ausgerichtet sind und dabei Zugriff auf die Daten des Verantwortlichen erhält (z.B. Rechenzentren) (Art. 28 Abs. 2, Abs. 4 DSGVO). Dienstleistungen die der Auftragsverarbeiter bei Dritten als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben und die nicht im Kernbereich auf eine Verarbeitung von personenbezogenen Daten ausgerichtet sind, sind hiervor ausgenommen. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Die nachfolgenden Regelungen finden sowohl für den Unterauftragsverarbeiter als auch für alle in der Folge eingesetzten weiteren Unterauftragsverarbeiter entsprechende Anwendung.

(2) Die Beauftragung weiterer Unterauftragsverarbeiter gemäß Art. 28 Abs. 4 DSGVO wird dem Auftragsverarbeiter hiermit allgemein genehmigt. Dies steht unter dem Vorbehalt, dass der Auftragsverarbeiter den Verantwortlichen immer mindestens 4 Wochen vor der Auslagerung über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern informiert (E-Mail ist ausreichend), wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Widerspricht der Verantwortliche der Beauftragung binnen der vorgenannten Frist nicht aus wichtigem Grund, gilt die Genehmigung des Verantwortlichen als erteilt.

(3) Die nachfolgenden Regelungen finden sowohl für den Unterauftragsverarbeiter als auch für alle in der Folge eingesetzten weiteren Unterauftragsverarbeiter entsprechende Anwendung.

(4) Der Verantwortlichen ist damit einverstanden, dass der Auftragsverarbeiter zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragsverarbeiters zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragsverarbeiter (verbundenes Unternehmen) vor Beauftragung dem Verantwortlichen schriftlich angezeigt werden (E-Mail ist ausreichend), sodass der Verantwortlichen bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

(5) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der **AVV-Anlage 4** aufgeführten Unternehmen als Unterauftragsverarbeiter für Teilleistungen für den Auftragsverarbeiter tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Verantwortlichen. Für diese Unterauftragsverarbeiter gilt die Zustimmung für das Tätigwerden als erteilt, sofern der Verantwortlichen einer Beauftragung von Unterauftragsverarbeitern allgemein zugestimmt hat.

(6) Der Auftragsverarbeiter muss Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen dem Verantwortlichen und dem Auftragsverarbeiter vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen. Ist der Auftragsverarbeiter im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragsverarbeiters in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Unterauftragsverarbeiter im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den beschriebenen Kontroll- und Überprüfungsrechten des Verantwortlichen. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Die Unterauftragsverarbeiter sind in jedem Fall in der **AVV-Anlage 4** aufzuführen.

(7) Durch schriftliche Aufforderung ist der Verantwortlichen berechtigt, vom Auftragsverarbeiter Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragsverarbeiters zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(8) Der Auftragsverarbeiter ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen (siehe Abs. 1 dieses Abschnitts) angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(9) Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters.

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Verantwortlichen hat den Auftragsverarbeiter unter dem Aspekt ausgewählt, dass dieser hinreichende Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Verantwortlichen hat das Recht, im Benehmen mit dem Auftragsverarbeiter regelmäßig Überprüfungen durchzuführen oder im Einzelfall durch 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 Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortlichen von der Einhaltung der Pflichten des Auftragsverarbeiters überzeugen kann (Dokumentationspflicht, z.B. technische Einrichtung; alle Vertraulichkeitsverpflichtungen von Personen, die Daten verarbeiten; alle Auftragsverarbeitungsverträge der Unterauftragsverhältnisse). Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen 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 des eingesetzten Informations-Sicherheits-Management-Systems (z.B. gem. ISO 27001).

§ 9 Berichtigung, Einschränkung und Löschung von Daten

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

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

(3) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt und sind streng untersagt. Hierfür bedarf es einer vorherigen schriftlichen (mindestens Textform) Genehmigung des Verantwortlichen. 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.

(4) Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Verantwortlichen – hat der Auftragsverarbeiter

a) sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,

b) erstellte Verarbeitungsergebnisse,

c) Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen

dem Verantwortlichen auszuhändigen oder auf Anweisung des Verantwortlichen datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Gleiches gilt für alle Daten, die Betriebs- oder Geschäftsgeheimnisse des Verantwortlichen beinhalten. Das Protokoll der Löschung ist auf Anforderung vorzulegen und mindestens 3 Jahre aufzubewahren.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen, jedoch mindestens 3 Jahre, über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

(6) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung (mindestens Textform) über die Kostentragung.

(7) Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

§ 10 Leistungsort

(1) Die konkreten Angaben zum Leitungsort sind in **AVV-Anlage 1** festgelegt.

(2) Der Verantwortliche stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Verantwortlichen geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt beim Auftragsverarbeiter.

(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU/EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Verantwortlichen schriftlich informiert.

(4) Sofern der Auftragsverarbeiter vom Verantwortlichen nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Verantwortlichen als erteilt.

(5) Wenn der Auftragsverarbeiter die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragsverarbeiter zuvor die schriftliche Zustimmung (mindestens Textform) durch den Verantwortlichen einholen.

(6) Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragsverarbeiter, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

(7) Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragsverarbeiter für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 11 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 12 Laufzeit und Kündigung

(1) Die Laufzeit des AV-Vertrages richtet sich nach der Laufzeit des entsprechenden Hauptvertrages. Der Verantwortliche kann den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß vom Auftragsverarbeiter gegen Datenschutzvorschriften oder gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder bewusst und unbegründet nicht ausführen will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Dies gilt insbesondere bei der Nichteinhaltung der Pflichten aus Art. 28 DSGVO.

(2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages, z. B. bei Beendigung des Hauptvertrages, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

AVV-Anlage 1: Gegenstand, Art, Zweck und Schutzniveau der betroffenen Daten

(1) Dieser Auftragsverarbeitungs-Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Hauptvertrag ergeben.

(2)

Art der Verarbeitung (detailliertere Information zum Verarbeitungsablauf): Der Auftragsverarbeiter stellt dem Verantwortlichen die Software Hero zur Nutzung über das Internet oder per App zur Verfügung und erbringt in diesem Zusammenhang Dienstleistungen, die in der Leistungsbeschreibung (Ziff. 2 AGB Sonepar Hero) beschrieben sind.			
Art der Daten	**Zweck der Datenerhebung, -verarbeitung und -nutzung**	**Kreis der Betroffenen**	**Schutzniveau der Daten**
Nutzerdaten (Vor- und Nachname, Rolle, E-Mail-Adresse (dienstlich), Telefonnummer (dienstlich), Mobilfunknummer (dienstlich), Profilbild, Berechtigungen, Standortdaten (App), IP-Adressen, Browserinformationen, Quellen	Support in der Verwaltung, Einrichtung und Anwendung der Software	Beschäftigte des Auftraggebers	Normal
Unternehmensstammdaten (Firma, Adressdaten, Kundennummer, Haupt-E-Mail-Adresse, Haupt-Telefonnummer, Webseite, Ansprechpartner, Zahlungsdaten)	Verwaltung von Kunden sowie Grundlage zur Rechnungsstellung	Kunden des Auftraggebers (B2B)	Normal
Endkundendaten (Vor- und Nachname, Position/Funktion, E-Mail-Adresse (privat), Telefonnummer (privat), Mobilfunknummer (privat), Website, Fax (privat), Geburtsdatum, Zahlungsdaten	Anwendung der Software, Interaktion zwischen Anwender der Software und Endkunden des Auftraggebers	Kunden des Auftraggebers (B2C)	Normal

(3) Leistungsort

Auftragsverarbeiter wird die vertraglichen Leistungen

☒ in Deutschland

☐ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR)

☐ in einem Drittland erbringen.

erbringen.

Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen

☒ in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR)

☐ in einem Drittland.

Erfolgt eine Leistungserbringung durch einen Unterauftragsverarbeiter in einem Drittland, bleibt der Auftragsverarbeiter zur Einhaltung der diesbezüglichen Vorgaben der DSGVO verpflichtet und weist dies auf Verlangen nach.

AVV-Anlage 2: Weisungsberechtigte und Datenschutzbeauftragter/ Ansprechpartner

Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet sie insbesondere die Einhaltung folgender Vorgabe:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt.

b) ☐ Auftragsverarbeiter ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.

c) ☐ Da Auftragsverarbeiter seinen Sitz außerhalb der Union hat, benennt er einen Vertreter nach Art. 27 Abs. 1 DSGVO in der Union.

Zur Erteilung von Weisungen betreffend die Auftragsdatenverarbeitung sind aufseiten des Verantwortlichen folgende Personen berechtigt:

Siehe registrierte Personen des Verantwortlichen in Hero Software

Zum Empfang von Weisungen betreffend die Auftragsverarbeitung sind aufseiten der Auftragsverarbeiter ausschließlich folgende Personen berechtigt:

Kundenservice für Hero Software erreichbar unter hero@sonepar.de

Beim Auftragsverarbeiter ist folgende Person als Datenschutzbeauftragte/r bestellt:

Die Kontaktdaten der/des Datenschutzbeauftragten sind unter https://www.sonepar.de/info/datenschutz einsehbar. Darüber hinaus ist eine Kontaktaufnahme jederzeit unter folgender E-Mail-Adresse möglich: datenschutzbeauftragter@sonepar.de.

Beim Verantwortlichen ist folgende Person als Datenschutzbeauftragte/r bestellt:

Sofern eine Verpflichtung zur Benennung eines Datenschutzbeauftragten für den Verantwortlichen besteht, siehe Datenschutzhinweise der Webseite des Verantwortlichen.

AVV-Anlage 3: Technische und organisatorische Maßnahmen

Standort: Sonepar Deutschland Information Services GmbH, Natorper Str. 7, 59439 Holzwickede (Unterauftragsverarbeiter 1)

1. Vertraulichkeit (Art. 32 Abs.1 lit. b DSGVO)

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

1.1.1 Büro

Technische Maßnahmen	Organisatorische Maßnahmen
● Alarmanlagen ● Zäune und Pforten mit Zeitsteuerung ● Bewegungsmelder ● Sicherheitsschlösser (Schlüsselkarte/Zertifikat) ● Chipkarten für verschlossene Bereiche ● Videoüberwachung	● Besucheranmeldung ● Besucherbücher und Besucherprotokolle ● Verpflichtung für Gäste, Ausweise zu tragen ● Empfangspersonal zur Personenkontrolle ● Sorgfältige Auswahl von Reinigungs- und Wachpersonal ● Zeitgesteuerte Zutrittskontrolle durch den Wachdienst ● Sicherheitszonen mit verschiedenen Zutrittsberechtigungen

1.1.2 Rechenzentrum

Technische Maßnahmen	Organisatorische Maßnahmen
● Alarmanlagen ● Zäune und Pforten mit Zeitsteuerung	● Besucheranmeldung

● Bewegungsmelder ● Sicherheitsschlösser (Schlüsselkarte/Zertifikat) ● Schließsysteme mit Codesperren ● Chipkarten für verschlossene Bereiche ● Videoüberwachung	● Besucherbücher und Besucherprotokolle ● Verpflichtung für Gäste, Ausweise zu tragen ● Empfangspersonal zur Personenkontrolle ● Sorgfältige Auswahl von Reinigungs- und Wachdienst ● Zeitgesteuerte Zutrittskontrolle durch den Wachdienst ● Sicherheitszonen mit verschiedenen Zutrittsberechtigungen ● Alarmmeldung bei unberechtigtem Zutritt zum Rechenzentrum

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
● VPN-Verbindung ● Verschlüsselung von Datenträgern und mobilen Endgeräten ● Einsatz automatischer, passwortgeschützter Bildschirmschoner nach 10 Minuten ● Firewall ● Anti-Viren-Software ● Mobile Device Management ● Zwei-Faktor Authentifizierung mit zeitlicher Gültigkeitsdauer ● Zertifikatsbasierte Zugangskontrolle für WLAN inkl. WPA2 Verschlüsselung ● Authentifikation mittels Passworteingabe	● Schlüsselregelungen (Zertifikatsbasiert) ● Zusätzliche Verschlüsselung auf Ordnerebene ● Passwortregeln inkl. Vorgaben für die Komplexität des Passwortes und zeitlicher Gültigkeitsdauer ● Vertrauenswürdiges Personal für die Bereiche Sicherheit und Reinigung ● Generierung von Benutzerprofilen ● Zuordnung von Benutzerrechten ● Zeitliche Sperrung nach mehrmaliger falscher Passworteingabe? ● Unterschiedliche Zugangsregelungen für Administratoren und Benutzer

● Zertifikatsbasierter Netzwerkzugang ausschließlich für registrierte Geräte (NAC)	

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
● Protokollierung der Zugriffe auf Anwendungen ● Datenschutzkonforme Vernichtung von Datenträgern (Akten, Laufwerke) ● Verschlüsselung von Datenträgern und mobilen Endgeräten ● Identifizierungs- und Authentifizierungssystem	● Passwortregeln ● Berechtigungskonzepte („Need to know“ Prinzip) ● Anpassung der Anzahl an Administratoren, die die volle Zugriffsberechtigung haben ● Datenvernichtung durch Dienstleister ● Datenschutzkonforme Passwortregeln ● Protokollierung von Zugriffen ● Sichere Aufbewahrung von Datenträgern ● Einsatz von Aktenvernichtern

1.4 Trennungskontrolle

Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist zu garantieren!

Technische Maßnahmen	Organisatorische Maßnahmen

● Verschlüsselung von Datensätzen, die aus demselben Zweck verarbeitet werden ● Klare Trennung der für verschiedene Zwecke gespeicherten Daten ● Trennung von Test-, Demo-, Release- und Produktivsystem	● Mandantentrennung ● Auf die jeweiligen Datensätze angepasste Datenbankrechte und Berechtigungskonzepte ● Steuerung über Berechtigungskonzept

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen
●	●

Hinweis: Es findet keine Pseudonymisierung statt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen

● Sichere VPN-Technologie ● E-Mail-Verschlüsselung ● Elektronische Signatur ● Verschlüsselung der Transportwege z.B. HTTPS, SFTP	● Anfertigung eines Verfahrensverzeichnisses ● Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen ● Kein physischer Transport von Daten

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
● Anfertigung eines Protokolls bezüglich der Eingabe, Veränderung und Löschung von Daten ● Digitales Berechtigungskonzept (z.B. Active Directory, SAP)	● Einrichtung und Verwendung von individuellen Benutzernamen ● Vergabe von Zugriffsberechtigungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

Technische Maßnahmen	Organisatorische Maßnahmen
● Doppelte IT-Infrastruktur ● Backups in unterschiedlichen Brandabschnitten ● Diebstahlsicherungen	● Alarmanlagen ● Erstellung von Backups der Daten ● Zyklus der Backups-Anfertigung ● Tests für Datenwiederherstellungen

● Klimatisierung des Serverraums durch eine Klimaanlage ● Feuer- und Rauchmelder ● Feuerlöscher ● Virenschutz ● Redundante Internetverbindung ● Redundante Stromversorgung ● Firewall/ IDS ● Monitoring	● Festlegung von Meldewegen ● Notfall-Management

3.1.1 Rechenzentrum

Technische Maßnahmen	Organisatorische Maßnahmen
● USV (Unterbrechungsfreie Stromversorgung) ● Wasser-, Temperatur, Feuer- und Rauchmelder ● Feuerlöscher ● Schutzsteckdosen ● Regelmäßige Belastungstest (z.B. Dieselgenerator)	● Alarmanlage ● Schutz des Serverraums vor Risiken, z.B. durch Hochwasser, Brände oder gefährlich platzierte Sanitäranlagen ● Pentests ● Regelmäßige Durchführung von Krisen/-Notfallübungen ●

3.2 Wiederherstellbarkeit

Maßnahmen, die die rasche Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust oder Beschädigung gewährleisten.

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

3.2.1 Rechenzentrum

Technische Maßnahmen	Organisatorische Maßnahmen

● Redundantes Rechenzentrum ● Redundante Datenleitung mit hoher Geschwindigkeit	● Backup Pläne ● Notfallkonzept/ Notfallplan

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Verfahren zur Regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO))

Technisch-organisatorische Maßnahmen zur Prüfung der Umsetzung datenschutzrechtlicher Vorgaben.

Technische Maßnahmen	Organisatorische Maßnahmen
● Pentests ● Regelmäßige Prüfung der Hardware (Lifecyc-le, Performance) ● Incident-Response-Management	● Regelmäßige technische Wartung ● Informations-/IT-Sicherheitskonzept ● Datenschutzkonzept ● Eskalationsverfahren für Notfälle ● Regelmäßige Audits (intern und extern) ● Regelmäßige Prüfung von Verträgen ● Regelmäßige interne Überprüfung / Aktualisierung der getroffenen Maßnahmen gemäß dem Stand der Technik (durch DSB, IT-Revision etc.) ● Benennen eines Datenschutzbeauftragten ● Benennen eines IT-Sicherheitsbeauftragten

4.2 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

Data Privacy by Design and by Default

Technische Maßnahmen	Organisatorische Maßnahmen
• Beschränkung der Angaben und weiteren Verwendung auf das notwendige Maß	• Auswahl von qualitativ hochwertiger Technik • Einhaltung von Branchenstandards • Regelungen zur Datenminimierung, Datensparsamkeit und Erforderlichkeit • Beschränkung der Speicherfrist • Beschränkung der Zugänglichkeit • Beschränkung des Umfangs der Verarbeitung der erhobenen Daten • Verwendung von Opt-In-Lösungen • Kennzeichnung von Pflicht- und Freiwilligen-Angaben

4.3 Auftragskontrolle

Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogenen Daten nur nach Weisung des Verantwortlichen verarbeitet werden (können)!

Technische Maßnahmen	Organisatorische Maßnahmen
•	• Sorgfältige Auswahl von Auftragsverarbeiter • Abschluss von AV-Verträgen, Standardvertragsklauseln, NDAs • Überprüfung der Datenvernichtung nach Auftragsende • Vertragsstrafen

	● Schriftliche Weisungen an Auftragsverarbeiter ● Vereinbarung von wirksamen Kontrollrechten bezüglich der Auftragsverarbeiter ● Regelmäßige und Dauerhafte Überprüfung von Auftragsverarbeiter

AVV-Anlage 4: Unterauftragsverarbeiter

Nr.	Name und Anschrift des Unterauftragsverarbeiters	Beschreibung der Teilleistungen	Ort der Leistungserbringung
1	Sonepar Deutschland Information Services GmbH, Natorper Str. 7, 59439 Holzwickede	IT-Service für Kundenverwaltung und Kommunikationssystem	Holzwickede
2	Hero Software GmbH, Göttinger Hof 9, 30453 Hannover	Service für die Anwendung Sonepar Hero	Hannover