Rahmen-Auftragsverarbeitungsvertrag
gemäß Art. 28 DSGVO (Datenschutz-Grundverordnung)

Mit dem Annehmen des Angebots der SEG System-EDV und Organisationsgesellschaft mbH (SEG) schließt der Auftraggeber die nachfolgende, von der SEG verbindlich zur Annahme durch den Auftraggeber angebotenen Rahmen-Auftragsverarbeitungsvertrag zur Verarbeitung personenbezogener Daten mit der

SEG System-EDV und Organisationsgesellschaft mbH, Borsteler Chaussee 49, 22453 Hamburg

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

§1 Vertragsgegenstand

Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung.

Die Beauftragung durch den Auftraggeber wird durch einen oder mehrere Hauptverträge bestimmt. Dies können z.B. Dienstleistungsverträge, Leistungsbeschreibungen oder beauftragte Angebote sein (nachstehend Hauptvertrag genannt).

Die konkrete Auftragsverarbeitung ergibt sich aus diesem Rahmen-Auftragsverarbeitungsvertrag (AVV) und der **Anlage 1** (allgemeine technische und organisatorische Maßnahmen) zusammen mit der **jeweiligen produktspezifischen Anlage 2**. Die Anlagen in Ihrer jeweils aktuellen Fassung sind unter www.seghamburg.de/avv abrufbar.

§2 Verantwortlichkeiten

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, 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 allein verantwortlich.

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

Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Es gelten die gesetzlichen Bestimmungen des Art. 82 DSGVO. Bei Widersprüchen zwischen anderen Vereinbarungen und diesem AVV geht die Regelung dieses AVV vor.

§3 Weisungsbefugnis des Auftraggebers

Die Weisungen sind vom Auftraggeber in schriftlicher Form oder in Textform zu erteilen, sofern Sie über die Regelungen dieses AVV hinausgehen. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber 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 Auftragnehmer, sowie vom Auftraggeber in schriftlicher Form oder in Textform zu dokumentieren. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen bestätigt der Auftraggeber im Nachgang unverzüglich (mind. Textform).

Die empfangsberechtigten Personen des Auftragnehmers sind unter datenschutz@seghamburg.de erreichbar.

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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§4 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, Daten auf dokumentierte Weisung des Auftraggebers zu verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit von Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der zuständigen Aufsichtsbehörde.

Hierzu gehören

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

Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der Daten Befugten zur Vertraulichkeit und falls erforderlich auf das Fernmeldegeheimnis verpflichtet haben. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Hauptvertrages fort.

Der Auftragnehmer verpflichtet sich, den Auftraggeber 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 relevante Informationen zur Verfügung zu stellen und Anfragen von Betroffenen an den Auftraggeber weiterzuleiten.

Der Auftragnehmer stellt auf Anfrage des Auftraggebers dem Auftragnehmer alle Angaben zur Verfügung, die zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DSGVO benötigt werden.

Eine Verarbeitung außerhalb der Räumlichkeiten des Auftragnehmers (z.B. mobiles Arbeiten) ist gestattet, sofern das vereinbarte Sicherheitsniveau nicht unterschritten wird.

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren 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 beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

Sofern die oben genannten Unterstützungsleistungen über das normale Maß hinausgehen, kann der Auftragnehmer beim Auftraggeber einen angemessenen Vergütungsanspruch geltend machen.

§5 Technische und organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen (**Anlage 1**) 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.

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c), Art. 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.

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 dem Auftraggeber mitzuteilen. Die Benachrichtigung über wesentliche Änderungen erfolgt an die E-Mail-Adresse, die der Auftraggeber dem Auftragnehmer vorab über die datenschutz@seghamburg.de mitgeteilt hat.

§6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Die Angaben zum Datenschutzbeauftragen sind in **Anlage 1** hinterlegt.

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

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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 von Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber 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 Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Sofern die oben genannten Unterstützungsleistungen über das normale Maß hinausgehen, kann der Auftragnehmer beim Auftraggeber einen angemessenen Vergütungsanspruch geltend machen.

§7 Unterauftragsverhältnisse

Ein Einsatz von Unterauftragnehmern ist dem Auftragnehmer unter Einhaltung der folgenden Regelungen gestattet:

Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen. Den Unterauftragnehmern ist im Wege eines Vertrags im Wesentlichen dieselben Pflichten aufzuerlegen, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit.

Die Verarbeitung von Daten des Auftraggebers außerhalb der EU/EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsdienstleistungen, Reinigungskräfte und Maßnahmen zur Wartung sowie zur Sicherstellung der Vertraulichkeit, Integrität & Verfügbarkeit.

Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu ergreifen.

Für die zum Zeitpunkt der Vertragsunterzeichnung in der jeweiligen **produktspezifischen Anlage 2** aufgeführten Unterauftragnehmer gilt die Zustimmung für das Tätigwerden als erteilt.

Der Auftragnehmer ist berechtigt, weitere Unterauftragnehmer unter den vorher genannten Bedingungen einzusetzen und informiert den Auftraggeber rechtzeitig über die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Die Benachrichtigung über den Einsatz neuer Unterauftragnehmer erfolgt an die E-Mail-Adresse, die der Auftraggeber dem Auftragnehmer vorab über die datenschutz@seghamburg.de mitgeteilt hat.

§8 Kontrollrechte des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichenden 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 Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer 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 Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen, sofern die untenstehenden Nachweise in begründeten Einzelfällen nicht ausreichend sein sollten.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers 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.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO oder aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutz-beauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren)
- eine geeignete Zertifizierung des eingesetzten Informations-Sicherheits-Management-Systems (z.B. TISAX, ISO 27001).

Für die Durchführung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

§9 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, 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.

Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer alle im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger sowie Daten dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers

datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht.

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

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

§10 Zurückbehaltungsrecht

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

§11 Vertraulichkeit

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- und Betriebsgeheimnissen sowie Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln.

Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur Freigabe durch die andere Partei – mindestens in Textform - als vertraulich zu behandeln.

§12 Sonstiges

Die Laufzeit dieses AVV richtet sich nach dem zugrundliegenden Hauptvertrag. Er kann nicht separat gekündigt werden. Soweit nach Beendigung des Hauptvertrages noch Verarbeitungen notwendig sein sollten, beispielsweise Übermittlungen an den Auftraggeber, so gilt die Laufzeit automatisch bis zur vollständigen Beendigung aller Verarbeitungsvorgänge.

Dieser AVV kommt automatisch mit der Antragsannahme des Hauptvertrags durch den Auftraggeber verbindlich zustande, er ist ohne separate Unterschrift gültig.

Die unten aufgeführten Anlagen sind zwingender Vertragsbestandteil.

Nebenabreden bestehen nicht. Solche müssen grundsätzlich in Schriftform separat vereinbart werden.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlagen

- Anlage 1: Übersicht der allgemeinen technischen und organisatorischen Maßnahmen
- Anlage 2: Produktspezifischer Zweck, Art der Daten, Kreis der Betroffenen, Unterauftragnehmer