

## **Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO**

zwischen

**Flughafen Stuttgart GmbH**

Flughafenstraße 32

70629 Stuttgart

- Verantwortliche, nachstehend Auftraggeber genannt -

und

- nachstehend Auftragnehmer genannt -

einzelnen auch als „Partei“ bzw. gemeinschaftlich als „Parteien“ bezeichnet

### **Präambel**

Die Parteien sind in Vertragsbeziehungen in Form eines

getreten (nachfolgend Hauptvertrag).

Im Bereich dieses Hauptvertrags erlangt der Auftragnehmer Zugang zu personenbezogenen Daten und verarbeitet personenbezogene Daten, für welche der Auftraggeber Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO ist. Der Auftragnehmer ist daher Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DS-GVO.

Vor diesem Hintergrund schließen die Parteien folgende Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO:

### **§ 1 Gegenstand und Dauer des Auftrags**

(1) Der Gegenstand des Auftrags ergibt sich aus

dem Hauptvertrag, auf welchen hier verwiesen wird;  
Anlage F, zu dieser Vereinbarung zur Auftragsverarbeitung.

- (2) Die Dauer dieses Auftrags entspricht der Laufzeit des Hauptvertrags.

## § 2 Konkretisierung des Auftragsinhalts

- (1) Zweck und Umfang der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret

im Hauptvertrag;  
in der **Anlage E**

beschrieben. Die personenbezogenen Daten werden vom Auftragnehmer nur in dem dort beschriebenen Umfang und ausschließlich zu dem dort geregelten Zweck verwendet.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland, auch durch einen Unterauftragnehmer des Auftragnehmers, außerhalb der EU / des EWR bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

- (2) Die Art der personenbezogenen Daten und die Kategorie der durch die Verarbeitung betroffenen Personen sind in **Anlage A**, in der jeweils gültigen Fassung, beschrieben.

## § 3 Technisch-organisatorische Maßnahmen

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Vereinbarung zur Auftragsverarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, 2 DS-GVO 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 DS-GVO zu berücksichtigen. Die Einzelheiten finden sich in **Anlage B**.

- (3) Der Auftraggeber ist sich darüber bewusst, dass die technischen und organisatorischen Maßnahmen der technischen Weiterentwicklung unterliegen. Der Auftragnehmer hat daher das Recht, angemessene Alternativmaßnahmen zu treffen, soweit dabei das vermittelte Schutzniveau nicht abgesenkt wird. Der Auftragnehmer hat den Auftraggeber über geplante technische Änderungen rechtzeitig zu informieren.

#### **§ 4 Berichtigung, Einschränkung und Löschung von Daten**

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

#### **§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung zur Auftragsverarbeitung gesetzliche Pflichten gem. Art. 28 bis 33 DS-GVO.

Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gem. Art. 38 und 39 DS-GVO ausübt. Der Datenschutzbeauftragte ist in **Anlage C**, in der jeweils gültigen Fassung, benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- b. Die Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in dieser Vereinbarung zur Auftragsverarbeitung eingeräumten Befugnisse, es sei denn, dass eine gesetzliche Verpflichtung zur Verarbeitung besteht. Der Auftragnehmer stellt sicher, dass die Regelungen dieser Vereinbarung zur Auftragsverarbeitung auch bei Verarbeitung von personenbezogenen Daten des Auftraggebers in Privatwohnungen von Beschäftigten (z.B. im Rahmen von Home-Office) gewährleistet ist.
- c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO: Einzelheiten in **Anlage B**, in der jeweils gültigen Fassung.
- d. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

- e. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f. 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 angemessen zu unterstützen.
- g. Der Auftragnehmer kontrolliert regelmäßig, mindestens jedoch alle 6 Monate, 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 Person gewährleistet wird. Der Auftragnehmer wird den Auftraggeber über die Kontrolle, deren Inhalt und das Ergebnis der Kontrolle schriftlich informieren.
- h. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieser Vereinbarung zur Auftragsverarbeitung.

## **§ 6 Unterauftragsverhältnisse**

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post- oder Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Unterauftragnehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der vom Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfungsunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

- (3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (5) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragnehmern gelten. In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
- (6) Der Auftraggeber stimmt der Beauftragung der in der **Anlage D** ausgeführten Unterauftragnehmern unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 - 4 DS-GVO zu.

## **§ 7 Kontrollrechte des Auftraggebers**

- (1) Der Auftraggeber hat das Recht, sowohl jährlich, als auch anlassbezogen Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:
  - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
  - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
  - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
  - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz).

- (4) Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

## **§ 8 Mitteilung und Unterstützung durch den Auftragnehmer**

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören unter anderem:

- a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

## **§ 9 Weisungsbefugnis des Auftraggebers**

- (1) Der Auftragnehmer wird als Auftragsverarbeiter nur im Rahmen der Weisungen des Auftraggebers tätig. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber nach Überprüfung bestätigt oder geändert wird.
- (3) Weisungen des Auftraggebers haben durch eine weisungsbefugte Person des Auftraggebers gegenüber einer zur Annahme von Weisungen berechtigten Person des Auftragnehmers stattzufinden. Die jeweils autorisierten Personen finden sich in **Anlage C**.

## § 10 Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien (insbesondere Back-Ups), soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschlussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) 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.

## § 11 Schlussbestimmungen

- (1) Für diese Vereinbarung zur Auftragsverarbeitung gelten die EU-Datenschutz-Grundverordnung (DS-GVO), das Bundesdatenschutzgesetz (BDSG), das jeweilige Landesdatenschutzgesetz (LDSG) sowie alle diese begleitenden bzw. ergänzenden gesetzlichen Regelungen in ihrer jeweils geltenden Fassung. Im Falle einer Änderung der Regelungen verpflichten sich die Parteien jeweils zur entsprechenden Anpassung dieser Vereinbarung zur Auftragsverarbeitung.
- (2) Änderungen und Ergänzungen dieser Vereinbarung zur Auftragsverarbeitung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung oder Abbedingung dieser Schriftformklausel. Der Vorrang der Individualabrede (§ 305b BGB) bleibt unberührt.
- (3) Das Schriftformerfordernis gilt nicht für die Aktualisierung der Anlagen, hier ist die Textform (auch per E-Mail) ausreichend. Jede Änderung der Anlagen benötigt für ihre Wirksamkeit die Bestätigung durch die jeweils andere Partei in Textform (auch per E-Mail). Änderungen der Anlagen dürfen nur von den, in **Anlage C** genannten, autorisierten Personen initiiert oder bestätigt werden.
- (4) Die Einrede des Zurückbehaltungsrechtes im Sinne von § 273 BGB wird in Bezug auf die Herausgabe von Daten und Datenträgern an den Auftraggeber ausgeschlossen.
- (5) Sollten einzelne Teile dieser Vereinbarung zur Auftragsverarbeitung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung zur Auftragsverarbeitung im Übrigen nicht. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt die Regelung, die dem von den Parteien mit der unwirksamen oder undurchführbaren Regelung Gewollten in rechtlicher zulässiger Weise wirtschaftlich am nächsten kommt. Dasselbe gilt für den Fall einer Lücke in dieser Vereinbarung zur Auftragsverarbeitung.

(6) Diese Vereinbarung zur Auftragsverarbeitung unterliegt deutschem Recht unter Ausschluss des UN-Kaufrechts (CISG). Als Gerichtsstand wird Stuttgart vereinbart.

(7) Sollte der Hauptvertrag Regelungen beinhalten, die vorliegender Vereinbarung zur Auftragsverarbeitung widersprechen, gilt die vorliegende Vereinbarung zur Auftragsverarbeitung als vorrangig.

**Beigefügte Anlagen:**

Anlage A

Anlage B

Anlage C

Anlage D

Anlage E

Anlage F

<b>Flughafen Stuttgart GmbH / Auftraggeber</b>	<b>Auftragnehmer</b>
<b>Ort:</b> Flughafen Stuttgart	<b>Ort:</b>
<b>Datum:</b>	<b>Datum:</b>
<b>Name:</b> <b>Orga-Bez.:</b>	<b>Name:</b>
<b>Rechtsverbindliche Unterschrift</b>	<b>Rechtsverbindliche Unterschrift</b>
<b>Name:</b> <b>Orga-Bez.:</b>	<b>Name:</b>
<b>Rechtsverbindliche Unterschrift</b>	<b>Rechtsverbindliche Unterschrift</b>