Datenschutzmanagement (DSMS) Richtlinie:

Datenschutzrechtliche Anforderungen an Externe

Revisionsverfolgung:

Revision	Datum
1.0	13.04.2022
1.1	31.01.2023

Inhaltsverzeichnis

I. Zweck und Ziel

Die Flughafen Stuttgart GmbH (nachfolgend auch nur als „**FSG**“ oder „**Auftraggeber**“ bezeichnet) legt großen Wert auf Datenschutz und Datensicherheit, insbesondere auf die Beachtung der Anforderungen der Datenschutz-Grundverordnung (DS-GVO) (z.B. Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO, Sicherheit der Datenverarbeitung nach Art. 32 DS-GVO oder Erfüllung der datenschutzrechtlichen Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO).

Zweck und Ziel dieser Richtlinie ist eine datenschutzkonforme Zusammenarbeit mit Fremdfirmen und die Einhaltung datenschutzrechtlicher Vorgaben an die bestellten Produkte, Anwendungen und Dienstleistungen (nachfolgend ggf. auch nur als „**IT-Leistungen**“ bezeichnet) sicherzustellen. Dies gilt insbesondere für den Einsatz bzw. die Lieferung von Hard- und/ oder Softwarekomponenten, die auch zur Verarbeitung personenbezogener Daten eingesetzt werden sollen.

II. Grundlegende Anforderungen

1. Auftraggeber und Auftragnehmer werden bei der Erbringung der Leistungen jeweils die auf sie anwendbaren Bestimmungen und Gesetze über den Datenschutz in der jeweils gültigen Fassung einhalten.

2. Im Rahmen des Auftrags (gleich welcher Art) hat der Auftragnehmer in der Zusammenarbeit mit dem Auftraggeber und bezüglich der von ihm zu erbringenden bzw. zu liefernden IT-Leistungen (egal ob Kauf und/oder Werkleistung und/oder Dienstleistung) insbesondere die nachfolgend nicht abschließend aufgezählten **allgemeinen Anforderungen an den Datenschutz und die Datensicherheit** zu erfüllen:

   2.1 **Einhaltung der Datenschutzgrundsätze nach Art. 5 DS-GVO** (vgl. Art. 5 Abs. 1 lit. a bis f DS-GVO), insbesondere:

   - Sicherstellung Rechtmäßigkeit / Transparenz;
   - Einhaltung der Zweckbindung;
   - Beachtung des Grundsatzes der Datenminimierung / Datensparsamkeit;
   - Gewährleistung der Richtigkeit;
   - Gewährleistung der Speicherbegrenzung;
   - Gewährleistung der Integrität und Vertraulichkeit (vgl. auch Ziff. 2.4 technischer und organisatorischer Datenschutz).

   2.2 **Einhaltung, Umsetzung und Wahrnehmung der Rechte der betroffenen Personen** (vgl. Kapitel III DS-GVO / Artt. 12 ff. DS-GVO), insbesondere:

   - Unterstützung zur Information der betroffenen Personen nach Art. 13, 14 DS-GVO (ggf. Bereitstellung von Mustertexten);
   - Umsetzung und ggf. Wahrnehmung aller Betroffenenrechte nach Art. 15 ff. DS-GVO;
   - Umsetzung der genannten Anforderungen mit Unterstützung jeder im Rahmen des Auftrags beteiligten Hard- und/oder Softwarekomponente (vgl. Ziff. 2.3 Grundprinzipien Privacy by Design und Privacy by Default) und mit Unterstützung des Auftragnehmers.

   2.3 **Einhaltung der Grundprinzipien Privacy by Design** (Datenschutz durch Technikgestaltung) **und Privacy by Default** (datenschutzfreundliche Voreinstellungen), vgl. Art. 25 DS-GVO, insbesondere:

   - Umsetzbarkeit kundenspezifischer Konfigurations- und Administrations-anforderungen in jeder beteiligten Hard- und/oder Softwarekomponente (z.B.

Abbildung von individuellen Aufbewahrungs- und Löschfristen, aktive Umsetzung von Datensparsamkeit usw.);

- Einhaltung und Darstellung der Einhaltung dieser Grundsätze ggf. bereits bei der Softwareentwicklung und auch bei den eingesetzten Hardwarekomponenten (z.B. Vorgehensmodell, Entwicklungsprozess, Schutzbedarfsanalyse, Berücksichtigung von Maßnahmen zum Stand der Technik, Berücksichtigung von Datenschutz-Anforderungen, Durchführung von Bedrohungsanalysen, ggf. Implementierung von internen Richtlinien, z.B. Entwicklerrichtlinie);
- Je nach eingesetzter bzw. zu liefernder Software- und/oder Hardwarekomponente müssen spezifische Besonderheiten, ggf. nach Rücksprache mit dem Auftraggeber, berücksichtigt werden, z.B. datenschutzrechtliche und betriebliche Anforderungen an die Nutzung.

2.4 Sicherstellung der Sicherheit der Verarbeitung im Sinne des Art. 32 DS-GVO (**Technischer und organisatorischer Datenschutz**), insbesondere:

- Sicherstellung von Integrität, Verfügbarkeit und Vertraulichkeit entsprechend einer durchgeführten Schutzbedarfsanalyse, ggf. nach Rücksprache mit dem Auftraggeber;
- Datensicherheit, Integrität und Vertraulichkeit, vgl. Art. 5 Abs. 1 lit. f und Art. 32 DS-GVO.

2.5 **Herstellung der datenschutzrechtlich erforderlichen Vertragslage**, insbesondere bei Vorliegen einer Konstellation einer Auftragsverarbeitung nach Art. 28 DS-GVO (Einzelheiten dazu sind auch in Abschnitt III geregelt).

2.6 **Schaffung eines angemessenen Datenschutzniveaus im Sinne der Art. 44 ff. DS-GVO** durch den Auftragnehmer im Falle von Drittlandübermittlungen, insbesondere auch unter Berücksichtigung des Urteils des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 Rechtssache C-311/18 („Schrems II“) zur Frage internationaler Datenübermittlungen.

Weitere Einzelheiten sind auch nachfolgend unter Abschnitt III. und Abschnitt IV. geregelt.

3. Der Auftragnehmer beachtet die durch den Auftraggeber zum Vertragsinhalt gemachten Sicherheitsanforderungen. Insbesondere gelten die Regelungen der ISMS Richtlinie Sicherheitsanforderungen an Externe des Auftraggebers.

III. Anforderungen an die Zusammenarbeit mit dem Auftragnehmer

1. Auftragsverarbeitungen oder gemeinsame Verantwortung

1.1 Verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber entweder selbst verantwortlich ist oder die der Auftraggeber für Dritte verarbeitet, muss er sich dabei an die geltenden datenschutzrechtlichen Bestimmungen (insbesondere an die Anforderungen der DS-GVO) halten.

1.2 Sofern Gegenstand der beauftragten Leistung zumindest auch die Verarbeitung personenbezogener Daten durch den Auftragnehmer ist, schließen der Auftraggeber und der Auftragnehmer vor der Verarbeitung von personenbezogenen Daten durch den Auftragnehmer eine Auftragsverarbeitungsvereinbarung (nachfolgend auch nur als „**AVV**“ bezeichnet). Vor diesem Hintergrund unterzeichnet der Auftragnehmer die vom Auftraggeber bereitzustellende Vereinbarung zur Auftragsverarbeitung samt Anlagen (nach entsprechender Ergänzung bzw. Konkretisierung dieser Vorlage).

1.3 Im Zuge des Abschlusses der AVV treffen die Parteien entsprechende angemessene technisch-organisatorische Maßnahmen (nachfolgend auch nur als „**TOM**“ bezeichnet).

Dabei sind jeweils mindestens die grundlegenden Anforderungen für die IT-Leistung aus dem Datenschutz- und dem Informationssicherheitsmanagementsystem des Auftraggebers, die Vorgaben gemäß der Artt. 28 und 32 DS-GVO und weitere auf den Auftragnehmer als Auftragsverarbeiter anwendbarer gesetzlicher Bestimmungen einzuhalten.

1.4 Sofern aufgrund der konkreten Konstellation ggf. erforderlich (d.h. wenn z.B. keine Auftragsverarbeitung vorliegt), wird der Vertragspartner mit der Flughafen Stuttgart GmbH eine Vereinbarung über die gemeinsame Verantwortlichkeit (sog. Joint Controller Vereinbarung, vgl. Art. 26 DS-GVO) abschließen.

2. **Anforderungen an das vom Auftragnehmer eingesetzte Personal**

2.1 Der Auftragnehmer hat dem Auftraggeber einen zuständigen Ansprechpartner zum Thema Datenschutz zu benennen und teilt dem Auftraggeber dessen Kontaktdaten mit.

2.2 Der Auftragnehmer verfügt, soweit gesetzlich erforderlich, über einen bestellten betrieblichen Datenschutzbeauftragten mit der erforderlichen Fachkunde und teilt dem Auftraggeber auf Anfrage dessen Kontaktdaten mit.

2.3 Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des Auftrags betraut sind, die auf den Auftragnehmer anwendbaren Bestimmungen über den Datenschutz beachten.

2.4 Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des Auftrags betraut sind, spätestens vor der erstmaligen Aufnahme der Tätigkeit entsprechend den einschlägigen gesetzlichen Bestimmungen auf das Datengeheimnis verpflichtet sind. Auf Verlangen und nach Wahl des Auftraggebers ist dem Auftraggeber entweder die Verpflichtung vorzulegen und/oder deren Vornahme schriftlich zu bestätigen.

2.5 Auf Verlangen des Auftraggebers sorgt der Auftragnehmer dafür, dass sich Personen, die von ihm mit der Bearbeitung oder Erfüllung des Auftrags betraut sind und dabei im besonderen Maße, in besonderer Weise (z.B. Remote-Zugriff) oder auf besonders sensible Daten Zugriff haben, zusätzlich gegenüber dem Auftraggeber zur Vertraulichkeit verpflichten. Hierfür wird der Auftraggeber eine Vorlage für eine entsprechende Verpflichtungserklärung bereitstellen.

IV. Anforderungen an Hard- und Softwarekomponenten bzw. IT-Systeme

1. Der Auftragnehmer gibt dem Auftraggeber alle relevanten, ggf. auch über die gesetzlichen Regelungen hinausgehende Sachverhalte bekannt, deren Kenntnis für den Auftraggeber aus Gründen des Datenschutzes und der Geheimhaltung erforderlich ist.

2. Soweit der Einsatz und/oder die Lieferung von Hard- und/oder Softwarekomponenten Gegenstand der beauftragten Leistung ist, müssen diese Komponenten den Auftragnehmer und den Auftraggeber bei den einzuhaltenden datenschutzrechtlichen Anforderungen (einschließlich der Anforderungen aus dieser Richtlinie) unterstützen, insbesondere durch eine datenschutzkonforme Konzeptionierung und Entwicklung sowie datenschutzfreundliche Voreinstellung.

3. Der Auftragnehmer hat hinsichtlich jeder etwaigen von ihm einzusetzenden und/oder zu liefernden Hard- und/ oder Softwarekomponente insbesondere die nachfolgenden nicht abschließend aufgezählten Anforderungen zu berücksichtigen:

3.1 **Einzelaccounts**

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen die Implementierung und die Verfügbarkeit von Einzelzugängen für die jeweiligen Berechtigten in technischer Hinsicht unterstützen (d.h. eigener Benutzername und eigenes, nur dem jeweiligen Berechtigten bekanntes Passwort).

Dies gilt insbesondere für den Fall, dass die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten ein datenverarbeitendes System bilden oder sich in ein solches einfügen. Ein solches muss grundsätzlich über Einzelzugänge für jeden Berechtigten verfügen. Gruppenkennungen darf es nur geben, sofern die Nachvollziehbarkeit einzelner Tätigkeiten von Benutzern und damit auch die Richtigkeit der personenbezogenen Daten anderweitig gewährleistet bleibt.

3.2 **Umsetzung der Passwort-Richtlinie**

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen die Umsetzung der Passwort-Richtlinie des Auftraggebers sicherstellen (können) bzw. die Umsetzung der Passwort-Richtlinie des Auftraggebers in technischer Hinsicht unterstützen. Für den Fall, dass die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten ein datenverarbeitendes System bilden oder sich in ein solches einfügen, muss deshalb gewährleistet sein, dass dieses System über die technischen Vorkehrungen verfügt, dass Passwörter zwangsläufig und turnusmäßig geändert werden müssen.

3.3 **Umsetzung des Vier-Augen-Prinzips**

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen die Umsetzung und Einhaltung des Vier-Augen-Prinzips - auch bei Änderungen an der Konfiguration/Einstellung durch die Administratoren - in technischer Hinsicht unterstützen.

Für den Fall, dass die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten ein datenverarbeitendes System bilden oder sich in ein solches einfügen, muss dies die Umsetzung und Einhaltung des Vier-Augen-Prinzips in technischer Hinsicht sicherstellen können und insbesondere über zusätzliche Sicherheitsvorkehrungen für den Fall verfügen, dass durch den Administrator ein Zugriff auf den Inhalt der im System gespeicherten personenbezogenen Daten erfolgt. Im System muss technisch angelegt sein, dass es für den administrativen Zugriff auf den Inhalt der im System gespeicherten personenbezogenen Daten die Freigabe durch einen zweite Person (z.B. zweiten Administrator oder die jeweils prozessverantwortliche Abteilung) braucht (bspw. in dem sich diese ebenfalls in das System einloggen und den Zugriff freigeben müssen) und administrative Tätigkeiten auf dem datenverarbeitenden System grundsätzlich durch einen zweiten Administrator freigegeben werden müssen.

3.4 **Umsetzung des Need-to-know-Prinzips**

Die im Rahmen des Auftrags vom Auftraggeber einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen in technischer Hinsicht unterstützen, dass Berechtigte nur auf Anwendungen, Speicher, Server und/oder Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen.

3.5 Logging / Protokollierungen

Die im Rahmen des Auftrags vom Auftraggeber einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen ein automatisches benutzerscharfes Logging bzw. eine automatisch benutzerscharfe Protokollierung über alle Aktivitäten auf den jeweiligen datenverarbeitenden Systemen in technischer Hinsicht unterstützen.

Für den Fall, dass die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten ein datenverarbeitendes System bilden oder sich in ein solches einfügen, braucht es ein benutzerscharfes Logging / Protokollierung jeder Tätigkeit auf dem datenverarbeitenden System, sobald sich ein Benutzer am datenverarbeitenden System einloggt. Dies gilt für rein administrative Tätigkeiten, ebenso wie für den Zugriff auf den Inhalt der im System gespeicherten personenbezogenen Daten.

3.6 Gewährleistung einer getrennten Verarbeitung

Die im Rahmen des Auftrags vom Auftraggeber einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen in technischer Hinsicht unterstützen, dass Daten, die zu unterschiedlichen Zwecken verarbeitet werden, getrennt gespeichert und weiterverarbeitet werden können.

3.7 Technische Lösung für die Offenlegung / Übermittlung von personenbezogenen Daten

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen in technischer Hinsicht unterstützen, dass personenbezogene Daten wenn, dann nur geschützt und dem Schutzbedarf angepasst etwaigen externen Empfängern zur Verfügung gestellt werden können.

3.8 Verfügbarkeit

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen in technischer Hinsicht unterstützen, dass Backups und Recovery möglich sind.

3.9 Löschung im Sinne der DS-GVO und differenziert einstellbare Löschfristen

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen differenziert einstellbare Zugriffs- und Löschfristen sowie das Löschen von personenbezogenen Daten im Sinne der DS-GVO in technischer Hinsicht unterstützen.

Für den Fall, dass die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten ein datenverarbeitendes System bilden oder sich in ein solches einfügen, muss insbesondere einstellbar sein, ob und wenn ja, unter welchen Bedingungen ein Benutzer wie lange auf die jeweiligen Daten (ohne weiteres) zugreifen kann.

3.10 Obligatorisches Self-Assessment (IT-Sicherheitsbewertung)

Für jede im Rahmen des Auftrags vom Auftragnehmer eingesetzte bzw. zu liefernde Hard- und/oder Softwarekomponenten ist jeweils vor der Implementierung ein nach den Vorgaben des Auftraggebers durchzuführendes Self-Assessment vorzunehmen.

3.11 Technische Standards und technische Sicherheit (Bedrohungsanalyse)

Für jede im Rahmen des Auftrags vom Auftragnehmer einzusetzende bzw. zu liefernde Hard- und/oder Softwarekomponente sind angemessene technische Standards entsprechend dem aktuellen Stand der Technik zu erfüllen.

Zur Wahrung der technischen Sicherheit ist eine angemessene Vorsorge durch eine Bedrohungsanalyse nach einem bewährten und anerkannten Modell (bspw. STRIDE-Modell oder IT-Grundschutz-Kompendium des BSI) sicherzustellen.

3.12 **Standards und Richtlinien für Leistungen aus dem Bereich des Cloud Computing**

Soweit der Auftragnehmer Leistungen aus dem Bereich des Cloud Computing erbringt (bspw. Leistungen in Form von Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Managed Cloud Services (MCS) und sonstige mit den vorgenannten Leistungsformen im Zusammenhang stehende Leistungen) erbringt er diese unter Einhaltung des bei Vertragsschluss jeweils aktuellen Cloud Computing Compliance Criteria Catalogue - C5 (Basiskriterien).

Zudem beachtet der Auftragnehmer die durch den Auftraggeber zum Vertragsinhalt gemachten Sicherheitsanforderungen, z.B. aus seiner Sicherheitsrichtlinie im Sinne des Mindeststandard(s) des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Nutzung externer Cloud-Dienste.

Sofern sich der Anforderungskatalog C5 (Basiskriterien) während der Laufzeit eines Vertrages ändert, wird sich der Auftragnehmer bemühen, auch die neuen bzw. geänderten Anforderungen innerhalb angemessener Frist zu erfüllen. Sollte der Auftragnehmer nicht innerhalb von zwölf Monaten (vorbehaltlich einer anderen vom Gesetzgeber vorgegebenen Umsetzungsfrist, die in jedem Fall einzuhalten ist) ab der Veröffentlichung des Nachfolgedokumentes gegenüber dem Auftraggeber auf Anforderung erklären, dass er die neuen und die geänderten Anforderungen erfüllt, hat der Auftraggeber ein mit einer Frist von einem Monat auszuübendes Sonderkündigungsrecht bezogen auf die betroffenen Leistungen. Der Auftraggeber verliert das Sonderkündigungsrecht nicht dadurch, dass er es nicht unverzüglich ausübt. Die Erneuerung eines etwaigen Testats erfolgt im üblichen Prüfungsturnus.

3.13 **Klassifizierung (Schutzbedarf)**

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzende bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen das erforderliche Minimum an Schutzbedarf gewährleisten. Der Auftraggeber wird diesen gemäß den Vorgaben des Datenschutzmanagementsystems des Auftraggebers ermitteln und dem Auftragnehmer insoweit die relevanten Sachverhalte bekannt geben.

Die daraus ableitbaren, sich ergebenden spezifischen Anforderungen und zu treffenden technischen und organisatorischen Maßnahmen (TOMs) werden im Rahmen des durchzuführenden Self-Assessments (s.o., Ziff. 3.10) konkretisiert.

3.14 **Wahrung der Betroffenenrechte**

Die im Rahmen des Auftrags vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten müssen die Einhaltung, Umsetzung und Wahrnehmung der Rechte betroffener Personen aus den Artt. 12 bis 23 DS-GVO in technischer Hinsicht unterstützen. Insbesondere müssen die jeweiligen Hard- und/oder Softwarekomponenten Funktionen ermöglichen, die genutzt werden können, um die zu einer Person gespeicherten Daten vollständig einsehen zu können.

Für den Fall, dass die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten ein datenverarbeitendes System bilden oder sich in ein solches einfügen, muss ein solches über eine entsprechende Funktion verfügen.

4. Die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten haben die vorbeschriebenen Anforderungen und Maßnahmen zu erfüllen.

Soweit einzelne Anforderungen und Maßnahmen durch die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten nicht selbst bzw. unmittelbar erfüllt werden können, hat der Auftragnehmer die betreffenden Anforderungen und Maßnahmen so zu berücksichtigen, dass deren anderweitige Erfüllung in technischer Hinsicht nicht durch die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten

verhindert wird. Dies gilt insbesondere für den Fall, dass die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten sich in ein datenverarbeitendes System einfügen sollen.

Soweit einzelne Anforderungen und Maßnahmen bereits in der vorhandenen und ggf. vom Auftraggeber bereitzustellenden Systemumgebung des Auftraggebers, in der sich die vom Auftragnehmer einzusetzenden bzw. zu liefernden Hard- und/oder Softwarekomponenten einfügen sollen, umgesetzt werden können oder umgesetzt werden müssen, ist dies gemeinsam mit dem Auftraggeber zu erörtern. In der Folge sind die betreffenden Anforderungen und Maßnahmen ggf. vom Auftragnehmer in Abstimmung mit dem Auftraggeber entsprechend anzupassen bzw. weiter zu konkretisieren.

V. Nachweispflichten und Dokumentation

1. Der Auftragnehmer muss hinreichend detailliert darlegen, welche personenbezogenen Daten er im Zuge des Auftrags verarbeitet und welche Schutzmaßnahmen er für diese Daten trifft.

2. Der Auftragnehmer verfügt über eine hinreichende Dokumentation über die Umsetzung der gesetzlichen Anforderungen, die der Auftragnehmer dem Auftraggeber auf Anforderung zugänglich macht.

3. Der Auftragnehmer hat dem Auftraggeber in geeigneter Form nachzuweisen, dass er und die von ihm zu erbringenden bzw. zu liefernden IT-Leistungen den Anforderungen aus dieser Richtlinie Rechnung tragen.

VI. Überprüfung der Umsetzung

1. Der Auftragnehmer verpflichtet sich,
   - in angemessenem Umfang regelmäßige interne Prüfungen in Bezug auf die Einhaltung und Umsetzung der datenschutzrechtlichen Anforderungen (einschließlich derjenigen aus dieser Richtlinie durchzuführen bzw. zu beauftragen;
   - dem Auftraggeber auf dessen Wunsch eine angemessene Überprüfung der Einhaltung und Umsetzung der datenschutzrechtlichen Anforderungen (einschließlich derjenigen aus dieser Richtlinie) im Rahmen von vor Ort Audits oder in Form angeforderter Nachweise zu gestatten und dabei nach besten Kräften zu unterstützen, wobei Vor-Ort-Audits in der Regel im Vorfeld angekündet werden und die betrieblichen Abläufe des Auftragnehmers nicht unverhältnismäßig beeinträchtigen dürfen.

2. Der Auftragnehmer gewährt die für eine Überprüfung notwendigen Zutritts-, Einsichts- und Auskunftsrechte und unterstützt im erforderlichen Ausmaß.

VII. Weitere Unterstützungs- und Mitwirkungspflichten

1. Im Rahmen des Auftrags hat der Auftragnehmer den Auftraggeber bei den hierbei einzuhaltenden datenschutzrechtlichen Anforderungen zu unterstützen. Insbesondere unterstützt der Auftragnehmer den Auftraggeber bei den Dokumentationsanforderungen der DS-GVO (insbesondere aus Art. 30 DS-GVO) und einer ggf. durchzuführenden Datenschutzfolgen-abschätzung nach Art. 35 DS-GVO.

2. Der Auftragnehmer gibt dem Auftraggeber alle relevanten, ggf. auch über die gesetzlichen Regelungen hinausgehenden Sachverhalte bekannt, deren Kenntnis für ihn aus Gründen des Datenschutzes erforderlich ist.

3. Der Auftragnehmer ist verpflichtet, Datenschutzpannen/-vorfälle in seiner Organisation, welche im Kontext der vertraglichen Vereinbarung stehen oder stehen können unverzüglich dem Auftraggeber zu melden.

VIII. Vertraulichkeit

Im Zusammenhang mit der Erbringung bzw. Durchführung von Leistungen für den Auftraggeber kann der Auftragnehmer Kenntnis von vertraulichen Informationen des Auftraggebers erhalten.

Vertrauliche Informationen sind alle dem Auftragnehmer von dem Auftraggeber in mündlicher, elektronischer, schriftlicher oder anderer Form zur Verfügung gestellten, offenbarten oder sonst zugänglich gemachten Informationen, z.B. Informationen über Planungen und Projekte, Organisation, Betriebsverfahren, Prozesse und Systeme, oder sonstiges operatives, technisches, wissenschaftliches, kommerzielles und finanzielles oder anderes Know-how. Vertrauliche Informationen in diesem Zusammenhang sind insbesondere auch personenbezogene Daten, die im Rahmen der geltenden Datenschutzgesetze geschützt sind.

Hinsichtlich dieser vertraulichen Informationen besteht ein besonderes Schutzbedürfnis des Auftraggebers. Deshalb verpflichtet sich der Auftragnehmer, mit dem Auftraggeber eine entsprechende Geheimhaltungsvereinbarung abzuschließen. Diese wird vom Auftraggeber zur Verfügung gestellt.

IX. Verhältnis dieser Richtlinie zu anderen Vertragsbestandteilen und Regelungen

1. Die Regelungen dieser DSMS Richtlinie lassen weitergehende gesetzliche und regulatorische Anforderungen unberührt.

2. Speziellere Regelungen (z.B. zum Datenschutz, zur Informationssicherheit, zur Vertraulichkeit oder zur Geheimhaltung) haben stets Vorrang vor allgemeineren Regelungen. Im Zweifelsfall gelten jedoch die nachfolgend genannten Regelungen in folgender Rangfolge:
   i. etwaige im Einzelfall getroffene, individuelle Vereinbarungen zum Datenschutz zwischen Auftraggeber und Auftragnehmer;
   ii. etwaige abgeschlossene Auftragsverarbeitungsvereinbarungen zwischen Auftraggeber und Auftragnehmer;
   iii. die Regelungen dieser DSMS Richtlinie.

Stand: 31.01.2023

Flughafen Stuttgart GmbH