Rahmenvereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

TA Triumph-Adler Deutschland GmbH

Südwestpark 23

90449 Nürnberg

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

Der Gegenstand und die Dauer des Auftrags sind in Anlage 3 spezifiziert.

2. Konkretisierung des Auftragsinhalts

(1) Umfang, Art und Zweck der Datenverarbeitung

Umfang, Art und Zweck der Datenverarbeitung sind in Anlage 3 spezifiziert.

(2) Ort der Datenverarbeitung

Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen. Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem Drittland. Erfolgt eine Leistungserbringung durch einen Unterauftragnehmer in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies auf Verlangen nach.

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 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.

(2) Der Auftragnehmer 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 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 zu dokumentieren.

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 dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Datenschutz-Ansprechpartner

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

i. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

ii. Die Kontaktdaten des Datenschutzbeauftragten lauten:

Data Protection Officer TA Triumph-Adler Gruppe, datenschutz@triumph-adler.net

iii. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO sowie Anlage 1.

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) 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.

(6) 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.

(7) Der Auftragnehmer kontrolliert regelmäßig 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.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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-/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.

☐ Eine Unterbeauftragung ist unzulässig.

☒ Der Auftraggeber stimmt der Beauftragung der in Anlage 2 genannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(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) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer 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 DSGVO 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 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 durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

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

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) 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 bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten 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 Ausschussmaterial. 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. Wirksamkeit der Vereinbarung

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

Ort, Datum, Unterschrift Auftragnehmer	Ort, Datum, Unterschrift Auftraggeber

Anlage 1 – Technisch-organisatorische Maßnahmen

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

(1) Zutrittskontrolle:
Personenkontrolle beim Pförtner/Empfang, Ausweisabgabe für betriebsfremde Personen, Begleitung von Betriebsfremden Personen im Gebäude, Manuelles Schließsystem, Sicherheitsschlösser, Schlüsselregelung/Protokollierung, personalisierte Zutrittsberechtigung für autorisierte Mitarbeiter mittels Transponder, Sicherung des Gebäudes nach Arbeitsschluss mittels Alarmanlage und Wachdienst

(2) Zugangskontrolle
Authentifikation mit Benutzer und Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts), automatische Sperrung (z.B. Kennwort oder Pausenschaltung), Einrichtung und Verwaltung von Benutzerstammdaten pro User, Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar, Einsatz von Anti-Viren-Software, Firewalls, VPN-Technologien

(3) Zugriffskontrolle
Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte), Auswertungen, Kenntnisnahme, Veränderung, Löschung, Anzahl Administratoren auf das Mindeste begrenzt, Passwortrichtlinien, Sichere Aufbewahrung von Datenträgern, Einsatz von Aktenvernichtung

(4) Trennungskontrolle
Interne Mandantenfähigkeit, Funktionstrennung (z.B. Admin-Rollen /Entwickler-Rollen/Allg. User), Produktion / Test, Berechtigungskonzept

(5) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Eine Pseudonymisierung findet nicht statt.

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

(1) Weitergabekontrolle
Prüfung der Rechtmäßigkeit der Weitergabe von Daten, Protokollierung, Transportsicherung, Datenschutzkonforme Vernichtung von Datenträgern

(2) Eingabekontrolle
Protokollierungs- und Protokollauswertungssysteme, Arbeitsanweisungen für Datenerfassung, Organisatorische Festlegung der Zuständigkeit für Eingaben von Daten, Verpflichtung auf das Datengeheimnis, Regelung der Zugriffsberechtigungen

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

(1) Verfügbarkeitskontrolle
Backup-Verfahren, Spiegeln von Festplatten, z.B. RAID-Verfahren, Unterbrechungsfreie Stromversorgung (USV), Getrennte Aufbewahrung, Virenschutz / Firewall, Notfallplan

(2) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)
Backup-Konzept, regelmäßige Prüfung und Testen der Wiederherstellungssysteme

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

(1) Datenschutz-Management

Verfahrensprüfung (Prüfung, Analyse), Monitoring von datenschutzmaßnahmen, Dokumentation von Datenschutzrisiken, Dokumentation der Verarbeitungssicherheit (ADV), Sensibilisierungsmaßnahmen für Mitarbeiter, Verfahren zur Meldung von Datenpannen

(2) Incident-Response-Management

Schulung von Mitarbeitern, wie auf Vorfälle zu reagieren ist, Dokumentation und Analyse eines Vorfalls zur Vermeidung von Wiederholungen, Datenschutz-Management-Organisation mit Datenschutz-Koordinatoren in den Fachbereichen

(3) Datenschutzfreundliche Voreinstellungen nach den Vorgaben des Auftraggebers (Art. 25 Abs. 2 DSGVO)

Löschkonzept (bei Wegfall des Zwecks)

(4) Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 2 – Subunternehmer

Unterauftragnehmer	Anschrift/Land	Leistung
Kyocera Document Solutions Inc.	1-2-28 Tamatsukuri, Chuo-ku, Osaka 540-8585, Japan	Unterstützung bei der Remote-Fehlerbehebung durch die Entwicklungsabteilung des Konzerns

Anlage 3 – Auftragsdokumentation

Auftragsdokumentation gemäß Kapitel 1 und 2 der Rahmenvereinbarung über Auftragsdatenverarbeitung zwischen **Auftraggeber** und **Auftragnehmer** vom

Datum des Auftrags	
Auftragsgegenstand	Der Gegenstand der Verarbeitung ist im Hauptvertrag geregelt.
Auftragsdauer	Die Dauer dieses Auftrags entspricht der Dauer der Geschäftsbeziehung.
Zweck, Umfang und Art der Datenverarbeitung	Erbringung von Dienstleistungen im Rahmen des Hauptvertrages, z.B. technischer Vor-Ort-Service, Remote-Support, kaufm. Abwicklung.
Kreis der Betroffenen - vom Auftraggeber zu ergänzen -	☒Kunden ☐Interessenten ☐Abonnenten ☒Beschäftigte ☒Lieferanten ☐Handelsvertreter ☒Ansprechpartner Sonstige:
Art der Daten - vom Auftraggeber zu ergänzen -	☒Personenstammdaten ☒Kommunikationsdaten (z.B. Telefon, E-Mail) ☒Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) ☒Kundenhistorie ☒Vertragsabrechnungs- und Zahlungsdaten ☐Planungs- und Steuerungsdaten ☒Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) Sonstige:
Besondere technisch-organisatorische Maßnahmen	keine
Besondere Weisungen	keine