# DATA PROCESSING AGREEMENT (DPA)

# -

# GEMÄSS ART. 28 DER EU-VERORDNUNG 2016/679

## ZWISCHEN

## Kunde (auch "DATENVERANTWORTLICHER")

## Und

## TecAlliance (auch "DATENVERARBEITER"),

im Folgenden gemeinsam die "Parteien" und einzeln eine "Partei".

Dieser Auftragsverarbeitungsvertrag ("**AVV**") ist Teil der Allgemeinen Geschäftsbedingungen von TecAlliance (der "**Vertrag**" oder die **"AGB"**)**.** Diese DPA tritt am Tag des Inkrafttretens in Kraft und bleibt für die Laufzeit der Vereinbarung in Kraft. Sofern in dieser DPA nichts anderes angegeben ist, bleiben die Bedingungen der Vereinbarung in vollem Umfang in Kraft und wirksam. Alle Klauseln oder Vereinbarungen, die sich auf die Privatsphäre oder den Datenschutz beziehen, die zuvor zwischen TecAlliance und dem Kunden in Bezug auf den Gegenstand dieser DPA abgeschlossen wurden, werden durch diese DPA ersetzt und durch diese ersetzt.

**PRÄAMBEL**

a. Der Kunde ist gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (im Folgenden "DSGVO") als "Datenverantwortlicher" für personenbezogene Daten qualifiziert; und

b. TecAlliance erbringt für den Kunden die in der Vereinbarung festgelegten Dienstleistungen (zusammen die "Dienstleistungen"), wie in der Vereinbarung beschrieben; und

c. Bei der Erbringung der Dienstleistungen gemäß der Vereinbarung verarbeitet TecAlliance personenbezogene Daten im Auftrag des Kunden in der Eigenschaft eines "Datenverarbeiters" gemäß der DSGVO; und

d. Die Parteien möchten gemäß Art. 28 DSGVO die Vorkehrungen für die Verarbeitung personenbezogener Daten (unten definiert) in diesem DPA im Rahmen der Dienste festlegen und verpflichten sich, die entsprechenden Bestimmungen in Bezug auf personenbezogene Daten einzuhalten, wobei jede Partei vernünftig und in gutem Glauben handelt.

**DAHER** vereinbaren die Parteien unter Berücksichtigung der hierin dargelegten gegenseitigen Versprechen und anderer guter und wertvoller Erwägungen, deren Erhalt und Zulänglichkeit hiermit anerkannt werden, in der Absicht, rechtlich gebunden zu sein, Folgendes:

## 1. Definitionen und Interpretation

1. Die Präambel sind integraler Bestandteil dieses DPA;

2. Verweise auf Abschnitte, Klauseln oder Absätze sind Verweise auf die Abschnitte, Klauseln oder Absätze dieser DPA, sofern nicht anders angegeben;

3. Wörter, die im Singular verwendet werden, schließen den Plural ein und umgekehrt, je nach Kontext;

4. Der Begriff "einschließlich" ist so auszulegen, als ob ihm die Worte "nur als Beispiel" folgen würden, um eine nicht erschöpfende Liste von Beispielen zu geben;

5. Alle großgeschriebenen Begriffe, die nicht in Abschnitt 1 oder anderweitig in dieser DPA definiert sind, haben die in der Vereinbarung festgelegte Bedeutung;

6. In dieser DPA haben die folgenden Begriffe und Ausdrücke die mit ihnen verbundene Bedeutung, wie unten dargelegt:

**"Verbundenes Unternehmen"** sind verbundene Unternehmen im Sinne der §§ 15 ff. AktG.

**"Verantwortlicher"** oder **"Datenverantwortlicher"** bezeichnet die Stelle, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten gemäß den Datenschutzgesetzen und -verordnungen gemäß Art. 4 Abs. 1 Nr. 7) der DSGVO entscheidet. Nur für die Zwecke dieser DPA und sofern nicht anders angegeben, umfasst der Begriff "Datenverantwortlicher" den Kunden, die Organisation und/oder die autorisierten verbundenen Unternehmen der Organisation.

"**Angemessenheitsbeschluss**" bezeichnet einen Beschluss der Europäischen Kommission auf der Grundlage von Art. 45 Abs. 3 der Europäischen Verordnung, durch den die Gesetze eines bestimmten Landes als geeignet angesehen werden, ein angemessenes Schutzniveau in Bezug auf die Verarbeitung personenbezogener Daten zu gewährleisten, wie es in den geltenden Rechtsvorschriften vorgesehen ist;

**"Vertrag"** bezeichnet die Bestellung oder den Vertrag, die einvernehmlich zwischen TecAlliance und dem Kunden geschlossen werden, zuzüglich der Allgemeinen Geschäftsbedingungen von TecAlliance (auch "AGB");

"**Anwendbares Recht**" bezeichnet die Europäische Verordnung und alle Gesetze und/oder Verordnungen, die die vor der Europäischen Verordnung geltenden Rechtsvorschriften umsetzen oder erlassen haben oder die aufgrund der vor der Europäischen Verordnung geltenden Rechtsvorschriften erlassen wurden und die aufgrund des Grundsatzes der Kohärenz weiterhin anwendbar sind, sowie alle verbindlichen Bestimmungen, die von den zuständigen Aufsichtsbehörden in dieser Angelegenheit erlassen wurden;

**"Kunde"** oder **"Sie"** ist eine natürliche oder juristische Person oder eine rechtlich verantwortliche Personengesellschaft, die bei der Durchführung eines Rechtsgeschäfts im Rahmen ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handelt;

**"Datenschutzgesetze und -vorschriften"** bezeichnet (a) die Gesetze der Europäischen Union oder der Mitgliedstaaten, einschließlich der DSGVO, in Bezug auf personenbezogene Daten der Organisation, die den EU-Datenschutzgesetzen unterliegen; (b) dem California Consumer Privacy Act von 2018 ("CCPA") in Bezug auf personenbezogene Daten der Organisation, für die die Organisation dem CCPA unterliegt, und (c) jedem anderen anwendbaren Recht in Bezug auf personenbezogene Daten der Organisation, für die die Organisation anderen Datenschutzgesetzen unterliegt.

**"Betroffene Person"** bezeichnet die identifizierte oder identifizierbare Person, auf die sich die personenbezogenen Daten beziehen, gemäß Art. 4 Abs. 1 Nr. 1 der DSGVO;.

"**Datum des Inkrafttretens**" bezeichnet das Datum, an dem dieses DPA unterzeichnet wird und zwischen den Parteien rechtsverbindlich und durchsetzbar wird. Sofern nicht anders angegeben, ist das Datum des Inkrafttretens das Datum, an dem die letzte Partei die Vereinbarung unterzeichnet hat. Ab diesem Datum treten alle hierin beschriebenen Rechte, Pflichten und Verantwortlichkeiten in Kraft;

**"Informationssicherheits- und Datenschutzdokument"** bezeichnet das Dokument, das die Maßnahmen beschreibt, die TecAlliance zum Schutz personenbezogener Daten ergreift, das hier zu finden ist.

**"Mitgliedstaat"** bezeichnet ein Land, das der Europäischen Union und/oder dem Europäischen Wirtschaftsraum angehört.

**"DSGVO"** bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

**"Personenbezogene Daten"** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, gemäß Art. 4 Abs. 1 Nr. 1 der DSGVO; Eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Bezugnahme auf eine Kennung wie einen Namen, eine Identifikationsnummer, Standortdaten, eine Online-Kennung oder auf einen oder mehrere Faktoren, die für die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person spezifisch sind.

"**Verletzung des Schutzes personenbezogener Daten**" oder "**Datenschutzverletzung**" bezeichnet eine Sicherheitsverletzung, die zu einer versehentlichen oder unrechtmäßigen Zerstörung, einem Verlust, einer Änderung, einer unbefugten Offenlegung oder einem unbefugten Zugriff auf personenbezogene Daten führt, die im Auftrag des für die Verarbeitung Verantwortlichen gemäß Art. 4 Abs. 1 Nr. 12) der DSGVO verarbeitet werden.

**"Verarbeitung"** oder **"Verarbeitungstätigkeit"** bezeichnet jeden Vorgang oder jede Reihe von Vorgängen, die mit personenbezogenen Daten durchgeführt werden, unabhängig davon, ob sie automatisiert sind oder nicht, wie z. B. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung,

Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung, gemäß Art. 4 Abs. 1 Nr. 2) DSGVO.

**"Auftragsverarbeiter"** oder **"Auftragsverarbeiter"** bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen gemäß Art. 4 Absatz 1 Nr. 8) der DSGVO verarbeitet;

"**Dienstleistungen**" bezeichnet die Dienstleistungen, die TecAlliance dem Kunden erbringt, wie in dem zwischen den Parteien geschlossenen Vertrag beschrieben;

**"Standardvertragsklauseln"** oder **"SCCs"** bezeichnet (i) die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Datenverarbeiter mit Sitz in Drittländern, die kein angemessenes Schutzniveau gewährleisten, wie in der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 4. Juni 2021 festgelegt, die hier verfügbar ist, in der aktualisierten Fassung, von Zeit zu Zeit von der Europäischen Kommission geändert, ersetzt oder ersetzt werden; oder (ii) wenn dies von Zeit zu Zeit von einer Aufsichtsbehörde für die Verwendung in Bezug auf eine bestimmte eingeschränkte Übertragung erforderlich ist, alle anderen Vertragsklauseln oder andere ähnliche Mechanismen, die von dieser Aufsichtsbehörde oder von den geltenden Gesetzen zur Verwendung in Bezug auf eine solche eingeschränkte Übertragung genehmigt wurden, in der von Zeit zu Zeit aktualisierten, geänderten, ersetzten oder ersetzten Fassung dieser Aufsichtsbehörde oder der Datenschutzgesetze und -vorschriften;

"**Unterauftragsverarbeiter**" bezeichnet einen Dritten, der nach den Anweisungen des Datenverarbeiters handelt, was bedeutet, dass er die personenbezogenen Daten von Personen im Auftrag des Datenverarbeiters verarbeiten kann. Ein Unterauftragsverarbeiter kann eine juristische Person, eine Behörde, eine Agentur oder eine andere Stelle sein.**"Aufsichtsbehörde"** bezeichnet eine unabhängige Behörde, die von einem EU-Mitgliedstaat gemäß der DSGVO eingerichtet wurde;

**"Technische und organisatorische Maßnahmen"** oder **"TOMs"** bezeichnet die Sicherheitsvorkehrungen und Kontrollen, die von einer Organisation implementiert werden, um die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten in Übereinstimmung mit den Datenschutzgesetzen und -vorschriften zu gewährleisten.

**"Union"** bezeichnet die Europäische Union.

## 2. Pflichten des für die Verarbeitung Verantwortlichen

Der für die Verarbeitung Verantwortliche erteilt dem Datenverarbeiter klare, vollständige und zeitnahe Anweisungen für die Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen und -vorschriften, einschließlich, aber nicht beschränkt auf die DSGVO und alle anderen relevanten nationalen oder internationalen Gesetze. Alle Anweisungen müssen rechtmäßig und dokumentiert sein und mit dem Umfang und den Zwecken der im Rahmen dieser DPA vereinbarten Verarbeitungstätigkeiten übereinstimmen.

Der für die Datenverarbeitung Verantwortliche ist allein verantwortlich für:
a) Sicherstellung der Einhaltung aller Verpflichtungen gemäß den geltenden Datenschutzgesetzen und -vorschriften, einschließlich der Transparenz gegenüber den betroffenen Personen, Schaffung gültiger Rechtsgrundlagen für die Verarbeitung und Sicherstellung der Richtigkeit, Relevanz und Rechtmäßigkeit der personenbezogenen Daten, die dem Datenverarbeiter zur Verfügung gestellt werden;
b) Garantie, dass die an den Datenverarbeiter übermittelten personenbezogenen Daten angemessen, relevant und auf das für die beabsichtigten Verarbeitungszwecke erforderliche Maß beschränkt sind;
c) Unverzügliche Unterrichtung des Datenverarbeiters über Änderungen der Rechtsgrundlage für die Verarbeitung oder andere Umstände, die die Rechtmäßigkeit der Verarbeitungstätigkeiten beeinträchtigen können.

Sind zusätzliche Maßnahmen oder Änderungen der Verarbeitung erforderlich, um die Einhaltung der Vorschriften zu gewährleisten, so hat der für die Verarbeitung Verantwortliche unverzüglich:
a) Bereitstellung aktualisierter und detaillierter Anweisungen zu den Zwecken, Methoden und Verfahren für die Verarbeitung;

b) Zusammenarbeit mit dem Datenverarbeiter, um geeignete technische und organisatorische Maßnahmen zu identifizieren und umzusetzen;
c) die volle Verantwortung für das Versäumnis zu tragen, rechtzeitige, rechtmäßige oder angemessene Anweisungen zu erteilen, und für alle daraus resultierenden Nichteinhaltungen, Verzögerungen oder Verbindlichkeiten, die dem Datenverarbeiter entstehen.

Der Datenverarbeiter haftet nicht für Folgen, die sich aus ungenauen, unvollständigen oder rechtswidrigen Anweisungen oder Daten ergeben, die vom für die Verarbeitung Verantwortlichen bereitgestellt werden.

### 3. Pflichten des Datenverarbeiters

Bei der Durchführung der Verarbeitung im Auftrag des für die Verarbeitung Verantwortlichen muss der Auftragsverarbeiter:

1. Verarbeiten Sie personenbezogene Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen und -vorschriften, respektieren Sie die Rechte und Freiheiten der betroffenen Personen und ergreifen Sie angemessene Maßnahmen, um Vertraulichkeit und Integrität zu gewährleisten.
2. Führen Sie nur die Verarbeitungstätigkeiten durch, die zur Erfüllung der in der Vereinbarung genannten Zwecke erforderlich sind, und nur im Rahmen der dokumentierten und rechtmäßigen Anweisungen des für die Verarbeitung Verantwortlichen.
3. Stellen Sie sicher, dass die Verarbeitung in Übereinstimmung mit den Grundsätzen der Rechtmäßigkeit, Fairness, Transparenz, Datenminimierung und Genauigkeit erfolgt, soweit dies auf die Rolle des Datenverarbeiters anwendbar ist.
4. Nicht haftbar gemacht werden für Verarbeitungen, die in Übereinstimmung mit den Anweisungen des für die Verarbeitung Verantwortlichen durchgeführt werden, es sei denn, diese Anweisungen sind offensichtlich rechtswidrig und der Datenverarbeiter hat es versäumt, den für die Verarbeitung Verantwortlichen zu benachrichtigen.
5. Stellen Sie sicher, dass das Personal, das zur Verarbeitung personenbezogener Daten berechtigt ist, entweder vertraglich oder gesetzlich angemessenen Vertraulichkeitsverpflichtungen unterliegt.
6. Informieren Sie den für die Verarbeitung Verantwortlichen über alle beabsichtigten Änderungen an den Unterauftragsverarbeitern und räumen Sie ihm eine angemessene Frist für Einwände aus begründeten rechtlichen Gründen ein.
7. Stellen Sie sicher, dass jeder ernannte Unterauftragsverarbeiter vertraglich an materiell gleichwertige Datenschutzverpflichtungen gebunden ist, und bieten Sie ausreichende Garantien für die Einhaltung. Der Datenverarbeiter bleibt für die Leistung der Unterauftragsverarbeiter verantwortlich, es sei denn, Verstöße ergeben sich aus Umständen, die außerhalb seiner angemessenen Kontrolle liegen, und es wurde die gebotene Sorgfalt walten lassen.
8. Soweit technisch machbar und verhältnismäßig, angemessene Unterstützung zu leisten, um den für die Verarbeitung Verantwortlichen bei der Beantwortung von Anfragen betroffener Personen gemäß den Artikeln 15 bis 22 der DSGVO zu unterstützen. Der Datenverarbeiter antwortet nicht direkt, es sei denn, er wurde ausdrücklich schriftlich genehmigt und nur wenn dies erforderlich ist.
9. Führen Sie ein Verzeichnis der Verarbeitungstätigkeiten, wenn dies gemäß Artikel 30 Absatz 2 der DSGVO erforderlich ist.
10. Unterstützung des für die Verarbeitung Verantwortlichen auf Anfrage und auf Kosten des für die Verarbeitung Verantwortlichen bei der Erfüllung der Verpflichtungen aus den Artikeln 32 bis 36 der DSGVO, soweit diese Verpflichtungen in direktem Zusammenhang mit den Aktivitäten des Datenverarbeiters und den verfügbaren Informationen stehen.
11. Informieren Sie den für die Verarbeitung Verantwortlichen über alle wesentlichen Probleme, die sich aus den geltenden Datenschutzgesetzen ergeben, einschließlich behördlicher Anfragen oder bestätigter Beschwerden betroffener Personen, wenn diese Probleme in direktem Zusammenhang mit den im Rahmen dieser DPA durchgeführten Verarbeitungsaktivitäten stehen.
12. Auf schriftliche Anfrage und vorbehaltlich des geltenden Rechts können Sie personenbezogene Daten nach Abschluss der Verarbeitungstätigkeiten löschen oder zurückgeben. Der Datenverarbeiter kann Daten aufbewahren, wie in Abschnitt 12 dieser DPA dargelegt.
13. Zusammenarbeit mit Audits, die vom Datenverantwortlichen initiiert werden, wie in Abschnitt 13 dieses DPA dargelegt.
14. Benachrichtigen Sie den für die Verarbeitung Verantwortlichen, wenn nach seiner vernünftigen Meinung eine Anweisung gegen diese DPA oder geltende Datenschutzgesetze und -vorschriften verstößt. In solchen Fällen muss der für die Verarbeitung Verantwortliche innerhalb von sieben (7) Werktagen nach

Erhalt einer solchen Mitteilung rechtmäßige, klare und spezifische Anweisungen erteilen. Wenn der für die Verarbeitung Verantwortliche dies nicht tut, behält er sich das Recht vor, die entsprechenden Verarbeitungstätigkeiten auszusetzen, bis solche Anweisungen eingegangen sind, ohne dass eine Haftung für eine solche Aussetzung übernommen wird.

**4. Sicherheitspflichten (Art. 32 DSGVO)**

Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, die den Branchenstandards entsprechen und den Stand der Technik, die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigen. Diese Maßnahmen sollen ein dem Risiko angemessenes Sicherheitsniveau gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Änderung, unbefugter Offenlegung oder unbefugtem Zugriff auf personenbezogene Daten.

Der Datenverarbeiter wendet mindestens die in Anhang II beschriebenen Maßnahmen an, die im Dokument Dokument zur Informationsicherheit und zum Datenschutz beschrieben sind , das als vom für die Verarbeitung Verantwortlichen akzeptiert gilt. Diese Kennzahlen können von Zeit zu Zeit aktualisiert werden, um sich ändernde Risiken, Technologien und regulatorische Anforderungen widerzuspiegeln.

Auf begründete schriftliche Anfrage und auf Kosten des für die Verarbeitung Verantwortlichen unternimmt der Auftragsverarbeiter wirtschaftlich angemessene Anstrengungen, um den für die Verarbeitung Verantwortlichen bei der Erfüllung seiner Verpflichtungen gemäß den Artikeln 32 bis 36 der DSGVO zu unterstützen, soweit diese Verpflichtungen in direktem Zusammenhang mit den vom Auftragsverarbeiter durchgeführten Verarbeitungstätigkeiten stehen.

Der Datenverarbeiter muss autorisiertes Personal mit Zugriff auf personenbezogene Daten identifizieren und Zugriffsrechte auf der Grundlage der Grundsätze der geringsten Privilegien und des Need-to-know-Prinzips zuweisen. Wenn ein Zugriff auf die Systeme des für die Verarbeitung Verantwortlichen erforderlich ist, muss der Datenverarbeiter diesen Zugriff streng auf das für die Erfüllung der Vereinbarung erforderliche Maß beschränken und alle anwendbaren Zugriffsprotokolle einhalten.

Der Datenverarbeiter bewertet die mit der Verarbeitung verbundenen Risiken und implementiert geeignete Sicherheitsvorkehrungen wie Verschlüsselung und Pseudonymisierung, soweit dies möglich ist. Diese Maßnahmen müssen in einem angemessenen Verhältnis zum Risiko stehen und so konzipiert sein, dass sie die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste dauerhaft gewährleisten. Der Datenverarbeiter haftet nicht für Restrisiken, die trotz der Umsetzung angemessener und verhältnismäßiger Sicherheitsmaßnahmen gemäß Artikel 32 der DSGVO bestehen bleiben, sofern diese Maßnahmen angemessen, dem Risiko angemessen und branchenüblich sind.

**5. Systemadministratoren**

Der Datenverarbeiter benennt Systemadministratoren nur dann, wenn dies für die Durchführung der Verarbeitung im Rahmen dieser DPA erforderlich ist. Die Benennung muss auf einer angemessenen Bewertung der Erfahrung, Zuverlässigkeit und Kompetenz der Person beruhen und intern dokumentiert werden.

Der Datenverarbeiter führt eine interne Liste der benannten Systemadministratoren und überprüft diese regelmäßig. Auf begründete schriftliche Anfrage des für die Verarbeitung Verantwortlichen kann der Datenverarbeiter unter Berücksichtigung von Vertraulichkeit und Sicherheit eine Zusammenfassung der aktuellen Liste zur Verfügung stellen.

Der Datenverarbeiter führt regelmäßige interne Überprüfungen der Aktivitäten des Systemadministrators durch, um die Einhaltung der geltenden Datenschutzgesetze und -vorschriften sowie der Sicherheitsanforderungen sicherzustellen. Die Ergebnisse solcher Überprüfungen können auf begründete schriftliche Anfrage an den für die Verarbeitung Verantwortlichen weitergegeben werden, sofern dadurch die internen Sicherheitsprotokolle oder geschützten Informationen des Datenverarbeiters nicht beeinträchtigt werden.

**6. Datenschutzverletzung**

Der Datenverarbeiter unternimmt angemessene Anstrengungen, um den für die Verarbeitung Verantwortlichen unverzüglich zu benachrichtigen, sobald er Kenntnis von einer bestätigten Verletzung des Schutzes personenbezogener Daten erhält, die wahrscheinlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Die Benachrichtigung muss, soweit dies nach vernünftigem Ermessen verfügbar ist, relevante Informationen enthalten, um den für die Verarbeitung Verantwortlichen bei der Erfüllung seiner Verpflichtungen gemäß den geltenden Datenschutzgesetzen und -vorschriften zu unterstützen, einschließlich der Verpflichtung, die Aufsichtsbehörde innerhalb von 72 Stunden zu benachrichtigen.

Der Datenverarbeiter ist nicht dafür verantwortlich, die Schwere oder Meldepflicht des Verstoßes gemäß der DSGVO zu bewerten, was in der alleinigen Verantwortung des für die Verarbeitung Verantwortlichen liegt. Die Informationspflicht des Datenverarbeiters beschränkt sich auf das, was nach vernünftigem Ermessen verfügbar ist.

Auf Verlangen einer zuständigen Aufsichtsbehörde und sofern gesetzlich vorgeschrieben, stellt der Datenverarbeiter das Verzeichnis der im Auftrag des für die Verarbeitung Verantwortlichen durchgeführten Verarbeitungstätigkeiten zur Verfügung, sofern eine solche Offenlegung die Vertraulichkeitsverpflichtungen des Datenverarbeiters oder die internen Sicherheitsmaßnahmen des Datenverarbeiters nicht beeinträchtigt.

## 7. Kommunikationen

Sofern nicht anders vereinbart, erfolgt jede formelle Kommunikation des Datenverarbeiters an den Datenverantwortlichen im Rahmen dieser DPA per E-Mail an die vom Datenverantwortlichen für Datenschutzangelegenheiten angegebene Adresse: CorporatePrivacy@tecalliance.net. Der Datenverarbeiter kann sich auf die neuesten Kontaktinformationen verlassen, die vom für die Verarbeitung Verantwortlichen bereitgestellt werden, und ist nicht verantwortlich für Verzögerungen oder Ausfälle in der Kommunikation, die auf veraltete oder falsche Kontaktdaten zurückzuführen sind.

Der Datenverarbeiter behält sich das Recht vor, gegebenenfalls alternative sichere Kommunikationskanäle zu nutzen, einschließlich sicherer Portale oder verschlüsselter Nachrichten, sofern diese Kanäle die Vertraulichkeit und Integrität der übermittelten Informationen gewährleisten.

## 8. Anfragen von betroffenen Personen

Der Datenverarbeiter implementiert angemessene Verfahren und ergreift geeignete technische und organisatorische Maßnahmen, um den für die Verarbeitung Verantwortlichen auf Anfrage bei der Beantwortung von Anfragen betroffener Personen gemäß den Artikeln 15 bis 22 der DSGVO zu unterstützen. Eine solche Unterstützung wird nur in dem Umfang gewährt, in dem der Datenverarbeiter technisch dazu in der Lage ist, und die Anfrage bezieht sich direkt auf Verarbeitungstätigkeiten, die im Rahmen dieser DPA durchgeführt werden.

Wenn der Datenverarbeiter eine Anfrage einer betroffenen Person direkt erhält, leitet er, soweit möglich, die Anfrage innerhalb von zwei (7) Werktagen an den für die Verarbeitung Verantwortlichen weiter, ohne verpflichtet zu sein, ihre Gültigkeit zu prüfen oder der betroffenen Person zu antworten.

Der Datenverarbeiter antwortet nicht auf Anfragen betroffener Personen, es sei denn, der für die Verarbeitung Verantwortliche hat dies ausdrücklich schriftlich genehmigt und nur wenn dies erforderlich ist. In solchen Fällen handelt der Datenverarbeiter streng im Rahmen der Genehmigung und übernimmt keine Verantwortung für die Verpflichtungen des Datenverantwortlichen gemäß den geltenden Datenschutzgesetzen und -vorschriften.

Der für die Verarbeitung Verantwortliche bleibt allein verantwortlich für die Erfüllung der Rechte der betroffenen Person und für alle Folgen, die sich aus der Nichteinhaltung ergeben.

## 9. Unterauftragsverarbeiter

Der Datenverarbeiter kann Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Rahmen dieser DPA beauftragen, vorbehaltlich der vorherigen allgemeinen schriftlichen Genehmigung des Datenverantwortlichen. Der Auftragsverarbeiter informiert den Verantwortlichen über alle beabsichtigten Änderungen in Bezug auf die Hinzufügung oder den Austausch von Unterauftragsverarbeitern und räumt ihm eine angemessene Frist ein, um aus begründeten und dokumentierten rechtlichen Gründen Einspruch zu erheben. Einwendungen

müssen schriftlich erhoben werden und dürfen die Erbringung der Verarbeitung nicht unangemessen verzögern oder behindern.

Die Liste der autorisierten Unterauftragsverarbeiter ist in Anhang I enthalten und kann von Zeit zu Zeit aktualisiert werden. Der Auftragsverarbeiter stellt sicher, dass jeder Unterauftragsverarbeiter vertraglich an Datenschutzverpflichtungen gebunden ist, die den in diesem DPA festgelegten Verpflichtungen im Wesentlichen entsprechen, einschließlich geeigneter technischer und organisatorischer Maßnahmen in Übereinstimmung mit der DSGVO.

Der Datenverarbeiter bleibt für die Leistung seiner Unterauftragsverarbeiter im Rahmen dieser DPA verantwortlich. Der Datenverarbeiter haftet jedoch nicht für einen Verstoß eines Unterauftragsverarbeiters, wenn ein solcher Verstoß auf Umstände zurückzuführen ist, die außerhalb der angemessenen Kontrolle des Datenverarbeiters liegen, vorausgesetzt, dass der Datenverarbeiter bei der Auswahl, dem Onboarding und der Aufsicht des Unterauftragsverarbeiters wirtschaftlich angemessene Sorgfalt walten ließ.

## 10. Übermittlung personenbezogener Daten ins Ausland

Wenn personenbezogene Daten auch nur teilweise in Ländern außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeitet werden, die keinem Angemessenheitsbeschluss der Europäischen Kommission unterliegen, vereinbaren die Parteien, dass solche Übermittlungen den geltenden SCCs unterliegen, die von der Europäischen Kommission für die Übermittlung personenbezogener Daten in Drittländer angenommen wurden.

Wenn der Auftragsverarbeiter einen Unterauftragsverarbeiter mit Sitz in einem solchen Drittland beauftragt, stellt der Auftragsverarbeiter sicher, dass die Standardvertragsklauseln zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter ausgeführt werden und dass der Unterauftragsverarbeiter ausreichende Garantien bietet, um geeignete technische und organisatorische Maßnahmen in Übereinstimmung mit der DSGVO zu ergreifen.

Der Datenverarbeiter haftet nicht für die Nichteinhaltung der SCCs durch den Unterauftragsverarbeiter, es sei denn, der Datenverarbeiter hat es versäumt, bei der Auswahl und Einarbeitung des Unterauftragsverarbeiters die gebotene Sorgfalt walten zu lassen.

## 11. Dauer

Diese DPA ist an die zugrunde liegende Vereinbarung zwischen den Parteien geknüpft und deckt sich mit dieser. Er endet automatisch bei Ablauf oder Beendigung des Vertrags, unabhängig vom Grund, ohne dass eine gesonderte Ankündigung oder Maßnahme erforderlich ist.

Der Datenverarbeiter ist nicht verpflichtet, die Verarbeitungstätigkeiten nach Beendigung des Vertrags fortzusetzen, es sei denn, dies ist ausdrücklich nach geltendem Recht vorgeschrieben oder von beiden Parteien ausdrücklich schriftlich vereinbart. In solchen Fällen ist der Datenverarbeiter berechtigt, angemessene Gebühren für alle Verpflichtungen zur Verarbeitung oder Datenverarbeitung nach der Beendigung zu erheben. Alle zusätzlichen Verarbeitungs-, Support- oder Compliance-Bemühungen, die über den Geltungsbereich der Vereinbarung oder dieser DPA hinausgehen, erfordern eine separate schriftliche Vereinbarung und können mit zusätzlichen Gebühren verbunden sein.

Der Datenverarbeiter haftet nicht für Verzögerungen oder Folgen, die sich aus der Beendigung der Verarbeitungstätigkeiten ergeben, sofern eine solche Beendigung in Übereinstimmung mit diesem DPA und der zugrunde liegenden Vereinbarung erfolgt.

## 12. Beendigung

Bei Beendigung der Verarbeitungstätigkeiten durch den Datenverarbeiter, aus welchem Grund auch immer, muss der Datenverarbeiter:

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, an den für die Verarbeitung Verantwortlichen zurückzugeben oder auf schriftlichen Antrag ihre Löschung zu veranlassen;
2. in jedem Fall eine schriftliche Bestätigung der ergriffenen Maßnahme vorlegen, nur wenn der für die Verarbeitung Verantwortliche dies innerhalb einer angemessenen Frist verlangt.

Der Datenverarbeiter ist nicht verpflichtet, personenbezogene Daten zu löschen oder zurückzugeben, soweit die Aufbewahrung:

a) nach geltendem Recht erforderlich,
b) die für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind, oder
c) wenn sie durch berechtigte Interessen gerechtfertigt sind, sofern diese Daten weiterhin angemessenen Garantien unterliegen und nicht für andere Zwecke verarbeitet werden.

Der Datenverarbeiter stellt sicher, dass alle gespeicherten Daten weiterhin in Übereinstimmung mit den in diesem DPA beschriebenen technischen und organisatorischen Maßnahmen geschützt sind.

## 13. Überwachung

Der für die Verarbeitung Verantwortliche kann Audits des Datenverarbeiters ausschließlich zu dem Zweck durchführen, die Einhaltung dieses DPA und der geltenden Datenschutzgesetze und -vorschriften zu überprüfen. Eine solche Prüfung ist an folgende Bedingungen geknüpft:

1. Der für die Verarbeitung Verantwortliche muss mindestens dreißig (30) Arbeitstage im Voraus eine schriftliche Mitteilung machen, in der er den Umfang und den Zweck des Audits angibt.
2. Die Audits dürfen höchstens einmal pro Kalenderjahr durchgeführt werden.
3. Die Audits werden während der regulären Geschäftszeiten und in einer Weise durchgeführt, die den normalen Betrieb des Datenverarbeiters nicht stört oder die Vertraulichkeit anderer Kunden oder geschützter Informationen beeinträchtigt.
4. Der für die Verarbeitung Verantwortliche trägt alle Kosten und Aufwendungen im Zusammenhang mit der Prüfung, einschließlich aller internen Ressourcen, die der Auftragsverarbeiter zur Unterstützung der Prüfung benötigt, es sei denn, es wird eine wesentliche Nichteinhaltung festgestellt.
5. Der Datenverarbeiter behält sich das Recht vor, den Zugang zu sensiblen oder vertraulichen Informationen zu beschränken, die nicht in direktem Zusammenhang mit den Verarbeitungstätigkeiten stehen, die unter diese DPA fallen.

## 14. Entschädigung und Haftung

Jede Partei ist verpflichtet, ihren jeweiligen Verpflichtungen gemäß den geltenden Datenschutzgesetzen und -vorschriften und diesem DPA nachzukommen.

Jede Partei erklärt sich damit einverstanden, die andere Partei von allen direkten Schäden, Verlusten oder Verbindlichkeiten (einschließlich Ansprüchen Dritter) freizustellen und schadlos zu halten, die sich aus ihrem eigenen Verstoß gegen geltende Datenschutzgesetze und -vorschriften oder diesen DPA ergeben. Die Entschädigung erstreckt sich nicht auf indirekte, zufällige, Folge- oder Strafschäden, es sei denn, sie wurden durch grobe Fahrlässigkeit oder vorsätzliches Fehlverhalten verursacht.

Der für die Verarbeitung Verantwortliche erkennt an und stimmt zu, dass der Datenverarbeiter nicht für Verarbeitungstätigkeiten haftbar gemacht werden kann, die in Übereinstimmung mit den dokumentierten Anweisungen des für die Verarbeitung Verantwortlichen durchgeführt werden, es sei denn, diese Anweisungen sind offensichtlich rechtswidrig und der Datenverarbeiter hat es versäumt, den für die Verarbeitung Verantwortlichen schriftlich über eine solche Rechtswidrigkeit zu informieren.

Der Datenverarbeiter ist nicht verantwortlich für:

1. Überprüfung der Rechtmäßigkeit, Richtigkeit oder Angemessenheit der vom für die Verarbeitung Verantwortlichen bereitgestellten personenbezogenen Daten;
2. Beurteilung der Gültigkeit der Rechtsgrundlage für die Verarbeitung;
3. Sicherstellung der Einhaltung der Verpflichtungen des für die Verarbeitung Verantwortlichen gemäß den geltenden Datenschutzgesetzen und -vorschriften.

Diese Verantwortlichkeiten verbleiben ausschließlich beim Datenverantwortlichen.

Der für die Verarbeitung Verantwortliche erkennt ferner an, dass der Datenverarbeiter nicht für Schäden haftet, die sich daraus ergeben, dass der für die Verarbeitung Verantwortliche seinen Verpflichtungen gemäß den geltenden

Datenschutzgesetzen und -vorschriften nicht nachkommt, einschließlich, aber nicht beschränkt auf die Bereitstellung genauer, rechtmäßiger und vollständiger Anweisungen oder Daten.

Die Parteien erkennen an, dass die Haftung in Übereinstimmung mit Artikel 82 der DSGVO und dem anwendbaren Recht auszulegen ist. Die Gesamthaftung des Datenverarbeiters im Rahmen dieser DPA ist auf die gesamten Gebühren beschränkt, die im Rahmen der Vereinbarung in den zwölf (12) Monaten vor dem Ereignis, das den Anspruch begründet, gezahlt wurden, es sei denn, es wurde grobe Fahrlässigkeit oder vorsätzliches Fehlverhalten des Datenverarbeiters nachgewiesen oder anderweitig gesetzlich vorgeschrieben.

## 1. Anwendbares Recht – Gerichtsstand

Im Falle einer Streitigkeit, die sich aus oder im Zusammenhang mit dieser DPA ergibt, bemühen sich die Parteien zunächst um eine gütliche Beilegung der Angelegenheit innerhalb von sechzig (60) Werktagen ab dem Datum, an dem eine Partei die andere über die Streitigkeit informiert.

Wird innerhalb dieser Frist keine Lösung gefunden, und sofern nicht schriftlich etwas anderes vereinbart wurde, unterliegen alle Streitigkeiten den Bestimmungen der einvernehmlich abgeschlossenen Vereinbarung und der ausschließlichen Zuständigkeit der zuständigen Gerichte.

## Anhang I: Liste der Unterauftragsverarbeiter

**Fremdbearbeitungsbeziehungen**

Die vertraglich vereinbarte Verarbeitung bzw. die nachfolgend beschriebenen Leistungsbestandteile werden von einem Unterauftragsverarbeiter durchgeführt, konkret:

| Name und Anschrift des Subunternehmers | Beschreibung der Dienstkomponente(n) |
|---|---|
| Amazon AWS, 410 Terry Avenue North, Seattle, Washington 98109-5210 USA | Cloud-Hosting (DPA and SCCs) |
| Zendesk, 1019 Market Street, San Francisco, Kalifornien 94103, USA | Ticket-System (DPA and SCCs) |
| Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA | Cloud-Hosting (DPA und SCCs) |

**Anhang II: TOM**

**Technische und organisatorische Maßnahmen (gemäß Art. 32 Datenschutz-Grundverordnung)**

# 1 Vertraulichkeit

Gemäß Art. 32 Abs. 1 lit. b) DSGVO.

**Access control**

Kein unbefugter Zugriff auf Datenverarbeitungssysteme.

- Zum Beispiel mit Magnet- oder Chipkarten, Schlüsseln, elektrischen Türöffnern, Werkssicherheit oder einem Pförtner, Alarmanlagen, Videosystemen.
- Realisierte Maßnahmen:
  Zutrittskontrollverwaltung, magnetisches Token, Chipkarte, Pförtner, Videoanlage, Alarmanlage

**Access control**

Keine unbefugte Nutzung des Systems.

- Zum Beispiel mit: (sicheren) Passwörtern, automatischen Blockierungsmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.
- Realisierte Maßnahmen:
  Sichere Passwörter, automatischer Blockierungsmechanismus

**Access control**

Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen innerhalb des Systems.

- Zum Beispiel mit: Berechtigungskonzepten und bedarfsgerechten Zugriffsrechten, Zugriffsprotokollen.
- Realisierte Maßnahmen:
  Authentifizierungs- und Autorisierungskonzept, "Need-to-know"-Prinzip, funktionale Trennung zwischen Erlaubnis und Vergabe von Berechtigungen

**Kontrolle der Trennung**

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

- Zum Beispiel mit: Mandantenfähigkeit, Sandboxing.
- Realisierte Maßnahme:
  Mandantenfähigkeit, Trennung zwischen Test- und Produktivsystem

**Pseudonymisierung**

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten nicht mehr einer bestimmten Person zugeordnet werden können

ohne Hinzuziehung zusätzlicher Informationen, sofern diese zusätzlichen Informationen getrennt gespeichert werden und

vorbehaltlich geeigneter technischer und organisatorischer Maßnahmen (gemäß Art. 32 Abs. 1 lit. a) DSGVO; Art. 25 Abs. 1 DSGVO).

- Realisierte Maßnahmen:
  Pseudonymisierung

## 2 Integrität

Gemäß Art. 32 Abs. 1 lit. b) DSGVO.

**Steuerung des Getriebes**

Kein unbefugtes Lesen, Kopieren, Verändern oder Löschen während der elektronischen Übertragung oder des Transports.

- Zum Beispiel mit: Verschlüsselung, virtuellen privaten Netzwerken (VPN), elektronischer Signatur.
- Realisierte Maßnahmen:
  Verschlüsselung/VPN, TLS

**Eingabekontrolle**

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder gelöscht wurden.

- Zum Beispiel mit: Protokollierung, Dokumentenmanagement.
- Realisierte Maßnahmen:
  Logging

## 3 Verfügbarkeit und Kapazität

Gemäß Art. 32 Abs. 1 lit. b) und c) DSGVO.

**Verfügbarkeitskontrolle**

Schutz vor versehentlichem oder mutwilligem Untergang oder Verlust.

- Zum Beispiel mit: Backup-Strategie (online/offline; vor Ort/extern), ununterbrochener Stromversorgung (USV), Virenschutz, Firewall, Meldekanälen und Notfallplänen; schnelle Wiederherstellbarkeit).
- Realisierte Maßnahmen:
  Backup-Konzept, unterbrechungsfreie Stromversorgung, Disaster-Recovery-Plan, Malware-Schutz, Firewall

## 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Gemäß Art. 32 Abs. 1 lit. d); Art. 25 Abs. 1 DSGVO.

**Datenschutzmanagement**

- Realisierte Maßnahmen:
  Regelmäßige Auditierung

**Incident-Response-Management**

- Realisierte Maßnahmen:
  Prozess des Incident-Managements

**Datenschutz in den Standardeinstellungen**

Gemäß Art. 25 Abs. 2 DSGVO

- Realisierte Maßnahmen:
  Prozess zur Gewährleistung von Privacy-by-Design/Privacy-by-Default

**Job-Steuerung**

Keine Vertragsabwicklung im Sinne des Art. 28 DSGVO ohne eine entsprechende Weisung des Kunden.

- Zum Beispiel durch: klare Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, ausreichende Garantien im Vorfeld, Nachkontrollen.
- Realisierte Maßnahmen:
  Eindeutige Auftragsvergabe, formalisiertes Auftragsmanagement