# VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

gem. Art. 28 DSGVO

| | |
|---|---|
| zwischen | **ASC Technologies AG**<br>**Seibelstraße 2-4**<br>**63768 Hösbach**<br>**Deutschland**<br>– nachfolgend „Auftragnehmer (Auftragsverarbeiter)“ genannt – |
| und | **Firma**<br>**Straße**<br>**PLZ Ort**<br>**Land**<br>– nachfolgend „Auftraggeber (Verantwortlicher)“ genannt – |
| | sowie einzeln oder in ihrer Gesamtheit als „Partei(en)“ bezeichnet. |

## 1. Präambel

Diese Vereinbarung zur Auftragsverarbeitung (nachstehend “Vereinbarung”) ergänzt den zugrundeliegende Hauptvertrag und damit zusammenhängende Leistungsvereinbarungen in datenschutzrechtlicher Hinsicht. Sie gilt besitzt hinsichtlich ihres Regelungsgehaltes und gemeinsam mit ihren Anlagen (sofern zutreffend) Vorrang gegenüber allen anderen Verträgen, Vereinbarungen und Absprachen.

Diese Vereinbarung regelt die Umsetzung der gesetzlichen Anforderungen hinsichtlich 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, kurz „DSGVO“), Art. 4 Nr. 2 und Art. 28, des Bundesdatenschutzgesetzes vom 30. Juni 2017 („BDSG“) sowie anderer einschlägiger deutscher Rechtsvorschriften.

Die Auftragsverarbeitung („Dienstleistung“) findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des Art. 44 ff. DSGVO erfüllt sind (bspw. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, BCRs). Falls ein Unterauftragsverarbeiter beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in Abschnitt 5 dieser Vereinbarung.

Diese Vereinbarung beginnt mit Unterschrift des Auftraggebers. Die Parteien vereinbaren, dass zeitgleich mit Beginn dieser Vereinbarung zwischen den Parteien zu gleichem Sachverhalt etwaig bestehende Verträge zur Auftragsdatenverarbeitung einvernehmlich aufgehoben und durch diese vorliegende Vereinbarung ersetzt werden.

## 2. Gegenstand der Vereinbarung

| | |
|---|---|
| Zugrundeliegender Hauptvertrag: | Temporäre oder dauerhafte Überlassung von Softwarelizenzen, Servicevertrag oder Subskription eines ASC Cloud-Dienstes. |
| Beschreibung des Auftragsgegenstands: | Bei On-Premise Installationen und sogenannte “Cloud Solutions für Service Provider”: Durchführung von Installationen und Installationsunterstützungen. Überprüfung, Anpassung, Erweiterung und Umrüstung von Hard- und Softwaresystemen. Erfüllung von Serviceverträgen über mehrere organisatorischen Stufen (“1st – 2nd – 3rd Level”) zur Fehleridentifikation und Störungsbeseitigung. Softwarepflege durch Updates und Upgrades. Management von Bestandsdaten und Datenbanken auf Weisung des Auftraggebers.<br><br>Im Falle von ASC Cloud-Diensten: Bereitstellung, Betrieb und Betriebserhaltung ebendieses Dienstes im Rahmen der gewählten Subskription und innerhalb der Microsoft Azure Cloud. |
| Beginn und Dauer des Auftrages: | Allgemein: Gemäß Hauptvertrag, Leistungsvereinbarungen und Nutzungs-/Lizenzbedingungen.<br><br>Im Falle von ASC Cloud-Diensten: Während der Laufzeit der Subskription. |
| Umfang, Art und Zweck der vorgesehenen Verarbeitung: | Erhebung, Übermittlung und Auswertung von Protokolldateien (“Logfiles”) im Rahmen von Systemeingriffen Systemen des Auftraggebers oder dessen Kunden, die durch Vor-Ort Intervention oder mittels Zugriffes über Datenfernübertragung ("Remote Service") durchgeführt werden.<br><br>Diese Protokolldateien und weitere Systeminformationen, einschließlich der in Abschnitt 4.13 beschriebenen Servicedaten, werden zur Erfüllung des Auftragsgegenstandes benötigt. Sie können personenbezogene Kommunikations- und Protokolldaten sowie Zugriffs- und Berechtigungsinformationen enthalten.<br><br>Die Verarbeitung personenbezogener Telekommunikationsinhalte und andere Bestandsdaten, die auf den Systemen des Auftraggebers oder dessen Kunden mit den dort installierten Produkten des Auftragnehmers aufgezeichnet und ausgewertet wurden, findet nur auf ausdrückliche Weisung des Auftraggebers statt. |
| Datenkategorien: | Protokolldateien, System-/Zugriffs-/Berechtigungsinformationen, Telekommunikationsinhalte.<br><br>Firmen- und Kontaktdatensätze. |
| Kategorien betroffener Personen: | Beschäftigte, Kunden, Interessenten, Geschäftspartner, Lieferanten, öffentliche Institutionen. |

2.1 Der Auftraggeber gilt als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO und Art. 24 DSGVO. Er ist für die Einhaltung der einschlägigen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung, die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, die Wahrnehmung von Informationspflichten, die Erteilung von Auskünften und die Erfüllung von Löschbegehren, verantwortlich.

2.2 Der Auftragnehmer verpflichtet sich, die gesetzlichen Bestimmungen ebenfalls einzuhalten und den Auftraggeber bei den oben genannten Anforderungen auf Anfrage zu unterstützen.

2.3 Der Auftraggeber kann diese Vereinbarung jederzeit und ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des zugrundeliegenden Hauptvertrages oder dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will, gegen die DSGVO oder sonstige Datenschutzvorschriften verstößt oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

**3. Rechte und Pflichten des Auftraggebers**

3.1 Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich oder in einem dokumentierten elektronischen Format. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und entsprechend schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber stellt sicher, dass alle Aufträge und Teilaufträge – soweit sie nicht der Tabelle in Abschnitt 2 dieser Vereinbarung entsprechen – Angaben zu folgenden Punkten enthalten:

a) Gegenstand und Dauer der Verarbeitung

b) Art und Zweck der vorgesehenen Verarbeitung von Daten

c) Art der personenbezogenen Daten

d) Kategorien betroffener Personen

3.2 Der Auftraggeber hat das Recht, jederzeit Weisungen gegenüber dem Auftragnehmer zu erteilen. Weisungen haben schriftlich oder per E-Mail zu erfolgen, mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Der Auftraggeber hat – sollte er in der Prozesskette selbst Auftragsverarbeiter eines übergeordneten Verantwortlichen sein – auf Verlangen des Auftragnehmers eine Bestätigung ebendieses übergeordneten Verantwortlichen für kritische Weisungen wie Löschungen vorzulegen oder deren Vorliegen justiziabel und mit befreiender Wirkung für den Auftragnehmer zu bestätigen.

3.3 Sind die Weisungen des Auftraggebers nicht vom vertraglich vereinbarten Leistungsumfang umfasst, werden diese als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Im Übrigen gelten die Leistungsbeschreibungen und jeweiligen vertraglichen Vereinbarungen.

3.4 Weisungsberechtigte Personen des Auftraggebers und Weisungsempfänger beim Auftragnehmer („Ansprechpartner“) sind in der Anlage 1 genannt. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners einer Partei ist der anderen Partei schriftlich oder in einem dokumentierten elektronischen Format der Nachfolger bzw. ein Vertreter mitzuteilen. Falls Weisungen die bisherigen vertraglich getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei weitere Kalenderjahre aufzubewahren.

3.5 Der Auftraggeber trägt die Verantwortung dafür, dass die beim Auftragnehmer vorgehaltenen technischen und organisatorischen Maßnahmen (siehe auch Abschnitt 6) für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Der Auftraggeber ist daher berechtigt, sich vor Beginn der Auftragsverarbeitung und sodann in angemessenen Abständen von der Einhaltung der beim Auftragnehmer getroffenen Vorkehrungen sowie der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten durch Inspektionen zu überzeugen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis der Inspektionen ist dem Auftragnehmer schriftlich mitzuteilen.

3.6 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

3.7 Der Auftraggeber ist verpflichtet, alle im Rahmen dieser Vereinbarung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

**4. Rechte und Pflichten des Auftragnehmers**

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO). Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

4.2 Soweit Datenträger eingesetzt werden, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden diese besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

4.3 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

4.4 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO sowie bei erforderlichen Datenschutz-Folgenabschätzungen des Auftraggebers gem. Art. 35 DSGVO hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben auf Anforderung durch den Auftraggeber jeweils unverzüglich an die in der Anlage 1 genannten Verantwortlichen des Auftraggebers, insbesondere auch an den dortigen Datenschutzbeauftragten (DSB), weiterzuleiten. Der Auftragnehmer ist berechtigt, für diese Mitwirkungs- und Unterstützungsleistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

4.5 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

4.6 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Der Auftragnehmer verweist auskunftsberechtigte Personen und Betroffene bei nicht vorliegender Zustimmung des Auftraggebers unverzüglich an den Auftraggeber als Verantwortlichen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen (siehe Anlage 1) erteilen.

4.7 Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen und Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

4.8 Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und Art. 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 lit. f DSGVO). Meldungen nach Art. 33 oder Art. 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß Ziffer 3 dieser Vereinbarung durchführen.

4.9 Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen, Untersuchungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO. Dies gilt auch, soweit eine zuständige Behörde beim Auftragnehmer ermittelt.

4.10 Bei Änderungen im Betriebsablauf, etwa bei Hard- und Softwareaustausch, hat der Auftragnehmer dafür zu sorgen, dass keine Daten des Auftraggebers an Dritte weitergegeben werden bzw. dass diese vor der Weitergabe datenschutzkonformgelöscht wurden.

4.11 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – ausschließlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im erforderlichen und angemessenen Umfang selbst zu kontrollieren oder durch von ihm beauftragte Dritte kontrollieren zu lassen, insbesondere durch die Einholung von Auskünften sowie Inspektionen vor Ort (Art. 28 Abs. 3 lit. h DSGVO). Der Auftragnehmer sichert zu, soweit erforderlich, bei diesen Inspektionen unterstützend mitzuwirken. Der Auftragnehmer ist berechtigt, für die Erteilung von Auskünften und Hinnahme bzw. Unterstützung von Inspektionen eine angemessene Vergütung vom Auftraggeber zu verlangen.

4.12 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber vorab abzustimmen.

4.13 Im Rahmen der Bereitstellung des Dienstes generiert und verarbeitet der Auftragsverarbeiter verschiedene Arten von Betriebsdaten („Servicedaten“), die für den sicheren, stabilen und effizienten Betrieb des Dienstes erforderlich sind. Dazu gehören:

a) System- und Anwendungsprotokolle

Von der Anwendung und Infrastruktur generierte Protokolle, wie Zeitstempel, Systemereignisse, API-Aufrufe, Leistungsmetriken und Fehlermeldungen. Diese werden zur Überwachung des Systemzustands, zur Fehlerbehebung, zum Störungsmanagement und für interne Audits verwendet.

b) Audit-Trails und Sicherheitsprotokolle

Unveränderliche Aufzeichnungen von administrativen und sicherheitsrelevanten Aktionen innerhalb des Dienstes. Sie dienen der Rechenschaftspflicht, der Überprüfung der Compliance und der Erkennung von Sicherheitsvorfällen.

c) Aggregierte Nutzungsanalysen

Anonymisierte oder pseudonymisierte Statistiken über die gesamte Systemnutzung, aggregiert über alle Tenants. Diese werden ausschließlich für Produktverbesserungen, Ressourcenplanung und Serviceoptimierung verwendet.

d) Personenbezogene Daten innerhalb der Servicedaten

Soweit technisch erforderlich und unvermeidbar, können Servicedaten begrenzte Kategorien personenbezogener Daten enthalten, darunter Benutzerkennungen (z. B. Benutzernamen, IP-Adressen, E-Mail-Adressen) und Kontaktdaten, die in Supportanfragen enthalten sind. Diese Daten werden ausschließlich für Systemdiagnosen, Kundensupport, Untersuchung von Vorfällen und Compliance-Zwecke verarbeitet.

Der Auftragsverarbeiter stellt sicher, dass die Aufnahme personenbezogener Daten auf das für die oben genannten Zwecke unbedingt erforderliche Maß beschränkt ist und dass diese Daten den in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen unterliegen.

4.14 Der DSB des Auftragnehmers ist in Anlage 1 namentlich genannt, ein Wechsel ist dem Auftraggeber unverzüglich mitzuteilen.

4.15 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung dieser Vereinbarung fort. Der Auftragnehmer bestätigt, dass ihm die einschlägigen gesetzlichen Vorschriften, inklusive des Fernmeldegeheimnisses nach § 3 TTDSG, bekannt sind.

4.16 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit (i) mit den für sie maßgebenden Bestimmungen des Datenschutzes durch Schulungen gemäß Art. 39 Abs. 1 lit. b DSGVO vertraut macht; (ii) für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 lit. b und Art. 29 DSGVO); und (iii) die Einhaltung der Vertraulichkeitsbestimmungen geeignet überwacht.

4.17 Der Auftragnehmer hat dreißig (30) Tage nach Beendigung der Auftragsverarbeitung alle ihm im Rahmen der Auftragsverarbeitung überlassenen personenbezogenen Daten vollständig und unwiderruflich in allen Systemen des Auftragnehmers (einschließlich sämtlicher Vervielfältigungen, auch in Archivierungs- und Sicherungsdateien) zu löschen (Art. 28 Abs. 3 lit. g DSGVO). Im Zeitraum zwischen Beendigung der Auftragsverarbeitung und endgültiger Löschung stellt der Auftragnehmer dem Auftraggeber sämtliche im Auftrag verarbeiteten Daten gegen ein Entgelt zum sicheren Herunterladen zur Verfügung. Die datenschutzgerechte Löschung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

**5. Unterauftragsverhältnisse (Art. 28 Abs. 3 lit. d DSGVO)**

5.1 Zum Zeitpunkt des Inkrafttretens dieser Vereinbarung setzt der Auftragnehmer die in Anlage 1 benannten Unterauftragsverarbeiter ein.

5.2 Der Verantwortliche erteilt dem Auftragsverarbeiter die grundsätzliche Genehmigung, weitere Unterauftragsverarbeiter in Anspruch zu nehmen. Der Auftragsverarbeiter informiert den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragsverarbeiter. Der Verantwortliche kann gegen eine solche beabsichtigte Änderung innerhalb von vier (4) Wochen nach Zugang der Mitteilung schriftlich oder in einem dokumentierten elektronischen Format Einspruch erheben, verbunden mit einem Sonderkündigungsrecht.

5.3 Eine Beauftragung von Unterauftragsverarbeitern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (bspw. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, BCRs).

5.4 Der Auftragnehmer versichert, dass er Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung im Hinblick auf die von ihm getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig ausgewählt hat.

5.5 Die Vereinbarung mit dem Unterauftragsverarbeiter muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

5.6 Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer sinngemäß auch für Unterauftragsverarbeiter gelten, und haftet gegenüber dem Auftraggeber für deren Einhaltung.

5.7 Die Weiterleitung von Daten ist erst zulässig, wenn der Unterauftragsverarbeiter die Verpflichtung nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat. In der Vereinbarung mit dem Unterauftragsverarbeiter sind die Angaben insbesondere zu Umfang, Art und Zweck der Datenverarbeitung sowie bezüglich der Abschnitte 4.7 und 5.1 so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragsverarbeiters deutlich voneinander abgegrenzt werden.

**6. Werden mehrere Unterauftragsverarbeiter eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragsverarbeitern.Technische und organisatorische Maßnahmen (Art. 32 DSGVO i.V.m. Art. 28 Abs. 3 lit. c DSGVO)**

6.1 Für die Auftragsverarbeitung wird ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Maßnahmen das Risiko auf Dauer eingedämmt wird.

6.2 Die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen des Auftragnehmers gelten vom Auftraggeber als ausreichend genehmigt. Sie können vom Auftragnehmer im Zeitverlauf sinnvoll weiterentwickelt und modifiziert werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form abstimmen.

6.3 Soweit die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen den Anforderungen des Auftraggebers nicht mehr genügen, benachrichtigt er den Auftragnehmer unverzüglich. Der Aufwand für etwaige Nachbesserungen, die einen vernünftigen Umfang überschreiten, kann der Auftragnehmer dem Auftraggeber in Rechnung stellen.

6.4 Sämtliche Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Unterauftragsverarbeitern) sind für die Geltungsdauer dieser Vereinbarung und anschließend noch für drei (3) volle Kalenderjahre aufzubewahren; es sei denn, gesetzliche Regelungen für eine längere Aufbewahrungsfrist stehen dem entgegen.

**7. Sonstiges**

7.1 Diese Vereinbarung – gemeinsam mit den zutreffenden Anlagen – stellt die gesamte diesbezügliche Vereinbarung zwischen den Parteien dar; mündliche Nebenabreden sind nicht getroffen.

7.2 Alle Änderungen und Ergänzungen dieser Vereinbarung haben schriftlich zu erfolgen, dies gilt auch für die Änderung des Schriftformgebots.

7.3 Sollte eine der Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Die Parteien sind in einem solchen Fall verpflichtet, bei der Schaffung von Bedingungen mitzuwirken, die ein rechtsgültiges Ergebnis erzielen, das dem der unwirksamen Bestimmung wirtschaftlich am nächsten kommt. Das Vorstehende gilt entsprechend für die Schließung etwaiger Lücken in der Vereinbarung.

7.4 Diese Vereinbarung selbst unterliegt dem Recht der Bundesrepublik Deutschland.

Siganturseite folgt

Bestandteil dieser Vereinbarung werden folgende Anlagen:

Anlage 1: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, autorisierte Personen und Unterauftragsverarbeiter
Anlage 2: Sondervereinbarungen – bei Bedarf ergänzen

| Auftragnehmer (Auftragsverarbeiter) | Auftraggeber (Verantwortlicher) |
|---|---|
| **ASC Technologies AG**<br>**Seibelstraße 2-4**<br>**63768 Hösbach**<br>**Deutschland** | **Firma**<br>**Straße**<br>**PLZ Ort**<br>**Land** |
| Name: | Name: |
| Funktion: | Funktion: |
| Datum: | Datum: |
| Unterschrift: | Unterschrift: |

**1. Beschreibung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO**

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

e) Zutrittskontrolle

*Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, bspw. durch Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Automatisches Zutrittskontrollsystem mit Protokollierung.
- Primär Chipkarten- / Transponder-Schließsystem mit elektrischen Motor-Schlössern.
- Zusätzlich manuelles Schließsystem mit Sicherheitsschlössern sowie Regelung zur Ausgabe / zum Einzug der Schlüssel.

Der Zutritt betriebsfremder Personen ist reguliert:

- Sie erhalten in den Geschäftsräumen nur nach Anmeldung beim Empfang und Abholung durch einen Mitarbeiter Zutritt und werden ständig begleitet. Der Zutritt zu sicherheitskritischen Bereichen ist nicht möglich und erfolgt, sollte er sachlich notwendig werden, ausschließlich in ständiger Begleitung und unter Aufsicht berechtigter Personen.
- Durch bauliche Maßnahmen ist eine Trennung zwischen Publikums- und Beschäftigtenverkehr sichergestellt. Der Zutritt zu den Bereichen, die ausschließlich Beschäftigen vorbehalten ist, kann nur über ein protokollierendes Zugangskontrollsystem erfolgen.
- Reinigungspersonal ist nur während der Geschäftszeiten und damit unter Aufsicht tätig.

Sicherheitskritische Bereiche (bspw. Serverräume, Standort der USV) sind baulich gesichert, der Zutritt ist nur einem eng begrenzten Personenkreis möglich.

Alarmanlage / Einbruchmeldeanlage überwacht sicherheitsrelevante Zonen nach Scharfschalten (automatisch Mo-Fr von 22:00 – 06:00 Uhr sowie am Wochenende) über Infrarot-Bewegungsmelder und Videokameras. Die Alarmanlage ist 24/7 mit einem Wachdienst verbunden, im Falle einer Alarmierung erfolgt eine Aufschaltung über Kameras und Gegensprechanlage. Bei unzureichender Identifizierung erfolgt die Alarmierung der Polizei und einer Kontaktperson von ASC.

f) Zugangskontrolle

*Keine unbefugte Systembenutzung, bspw. durch sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Persönliche Berechtigungen, beschränkt auf das zur Aufgabenerfüllung notwendige Maß („need-to-know“ Prinzip).
- Einsatz von personenbezogenen Benutzernamen in Microsoft Azure Active Directory-gehosteten Benutzerkonten.
- Authentifikation mit Benutzername / Passwort. Single-Sign-On an Workstations und Servern nicht möglich.
- User- und systemabhängige Zwei-Faktor-Authentifizierung, wird über dediziertes Smartphone erzwungen.
- Passwortrichtlinie gem. Vorgaben des BSI (Länge, Komplexität, Wechselfrequenz, Historie).
- Zuordnung von Benutzerprofilen zu IT-Systemen (Rollentrennung).
- Einsatz einer Hardware-Firewall, zusätzlich Software-Firewall auf allen Workstations und Servern.
- Einsatz von VPN-Technologie (AES-256-CBC, 2048 bit).
- Einsatz von aktiven Intrusion-Prevention-Systemen (Firewall).
- Bedarfsweise Verschlüsselung von mobilen Datenträgern (mind. AES-256 Hardwareverschlüsselung oder Bitlocker-to-go).
- Verschlüsselung von Datenträgern in Laptops (Full-Disk-Encryption über SSD-Firmware bzw. Microsoft Windows Bitlocker).
- Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum Fernlöschen).
- Bildschirmsperren, manuell oder erzwungen (Voreinstellung zehn Minuten).
- Organisationsanweisung zur sicheren Aufbewahrung von Dokumenten und mobilen Datenträgern.

g) Zugriffskontrolle

*Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, bspw. durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Persönliche Berechtigungen, beschränkt auf das zur Aufgabenerfüllung notwendige Maß („need-to-know“ Prinzip).
- Verwaltung der Rechte durch besonders verpflichtete Systemadministratoren nach dem 4-Augen-Prinzip.
- Anzahl der Administratoren auf das „Notwendigste“ reduziert.
- Passwortrichtlinie gem. Vorgaben des BSI (Länge, Komplexität, Wechselfrequenz, Historie).
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Sichere Aufbewahrung von Datenträgern.
- Bedarfsweise Verschlüsselung von Datenträgern.
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399), Protokollierung.
- Ordnungsgemäße Vernichtung von Papier (Einsatz von Aktenvernichtern bzw. Dienstleistern), Protokollierung.
- Einsatz von Anti-Viren-Software.
- Implementierung einer „Clean Desk Policy“.

h) Trennungskontrolle / Verwendungskontrolle

*Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, bspw. durch Mandantenfähigkeit, Sandboxing.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Logisch getrennte Speicherung auf denselben Systemen / Mandantentrennung.
- Falls erforderlich, getrennte Speicherung auf gesonderten Datenträgern.
- Trennung von Produktiv- und Testsystemen.
- Trennung von Produktiv- und Testsystem-Netzwerk.

i) Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

*Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Möglichkeit zur Verarbeitung von Daten in pseudonymisierter/anonymisierter Form.
- Trennung der Zuordnungsdatei und Aufbewahrung auf einem getrennten, abgesicherten System / Datenträger.
- Autorisierung zur Rückbeziehung der Pseudonyme anhand separater Zugriffsberechtigungen.
- Geeignete Kontrollen zur Überprüfung der Wirksamkeit.
- Weitere Angaben zur Verschlüsselung für den (elektronischen) Transport siehe Weitergabekontrolle (siehe Ziffer 1.1. d).
- Verschlüsselungsverfahren bei Speicherung in einem Datenbank-Container.
- Verschlüsselung auf Basis einschlägiger Standards (bspw. RSA, AES-256 Bit).
- Aufzeichnungsdaten in Lösung ASC Recording Insights können alternativ auch mittels eines kundeneigenen Azure-Keys (BYOK) verschlüsselt werden.

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

a) Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, bspw. durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Einrichtung von festen "Site-to-Site VPNs".
- Verschlüsselte Datenübermittlung (z. B. via https:// oder SFTP).
- E-Mail-Verschlüsselung nach aktuellem TLS Standard, soweit auf Gegenseite technisch möglich. Postfächer gehostet in Microsoft Office 365 Tenant.
- Verschlüsselung externer Datenträger wie Festplatten, CDs, USB-Sticks (mind. AES-256 Hardwareverschlüsselung oder Bitlocker-to-go).
- Protokollierung der Verbindungsdaten bei Datenübertragungen.
- Festlegung befugter Personenkreise für unterschiedliche Sachverhalte (Rollentrennung).
- Beim physischen Transport: Sichere Transportbehälter / -verpackungen sowie sorgfältige Auswahl von Transportunternehmen und Transportpersonal.

a) Eingabekontrolle

*Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, bspw. durch Protokollierung, Dokumenten-Management.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Systeminterne Protokollierung der Eingabe, Änderung und Löschung von Daten (Omnitracker).
- Festgelegte Zuständigkeiten in einem Berechtigungskonzept, inklusive Prozessdokumentation zur Vergabe von Rechten, Eingabe, Änderung und Löschung von Daten im Rahmen des ASC Multi-Management Systems.
- Nachvollziehbarkeit durch personenbezogene Benutzernamen / Passwörter.

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

a) Verfügbarkeitskontrolle

*Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, bspw. durch Backup-Strategie (online / offline; on-site / off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Erstellung eines Backup- und Recovery-Konzepts.
- Regelmäßige Sicherung von Systemzuständen.
- Regelmäßige Sicherung von Dateibeständen.
- Regelmäßige Sicherung von Datenbanken.
- Aufbewahrung von Datensicherungen an einen sicheren, ausgelagerten Ort, in feuer- und wassergeschützten Datensicherheitsschränken; die Tresore für die Lagerung von Datensicherungen haben Schutzklasse S 60 DIS.
- Aufbewahrung von Datensicherungen in einem anderen Brandabschnitt.
- Erstellung eines Notfallplans / -konzepts.
- Regelmäßige Aktualisierung von Softwareständen.

- Unterbrechungsfreie Stromversorgung (USV) und Überspannungsschutz.
- Klimaanlage in Serverräumen.
- Geräte zur Überwachung von Temperatur, Feuchtigkeit sowie CO / $CO^2$ in Serverräumen.
- Schutzsteckdosenleisten in Serverräumen.
- Feuer- und Rauchmeldeanlagen.
- Feuerlöschgeräte in Serverräumen.
- Alarmmeldungen bei unberechtigten Zutritten oder Zutrittsversuchen zu Serverräumen, siehe auch Ziffer 1.1 a)
- Serverräume nicht unter sanitären Anlagen oder Wasser- oder Abflussleitungen.

b) Belastbarkeit der Systeme

*Das Risiko durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang aufgrund von Systemüberlastungen oder -abstürzen ist zu reduzieren.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Überwachung der Betriebsparameter, Nutzung der Dienste und Auslastung der Systeme.
- Notfallkonzept.
- Nutzung redundant ausgelegter Systeme / Komponenten (Hardware).
- Herstellerdiversifizierung bei Schutzkomponenten (Hard- und Software).
- Maßnahmen zur Abwehr von Angriffen (z. B. Virenscanner, Firewall).
- Regelmäßige Prognose der zukünftigen Nutzung und rechtzeitige Anpassung der Kapazitäten der Systeme.
- Auslegung der Speicher-, Zugriffs- und Leistungskapazitäten der Systeme und Dienste bei geplanten oder prognostizierten Spitzenbelastungen.
- Einsatz fehlertoleranter Systeme.

c) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Wiederherstellung nach Backup- und Recovery-Konzept.
- Testen von Datenwiederherstellungen.

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

a) Datenschutz-Management

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Verbindliche unternehmensweite Datenschutzleitlinie.
- Datenschutz-Verfahrensanweisung innerhalb des ASC Multi-Management Systems.
- Regelmäßige interne Datenschutz-Audits.
- Kontrollsystem, das unberechtigten Zugriffe oder Zugriffsversuche blockiert.
- Verzeichnis von Verarbeitungstätigkeiten ist vorhanden und auf dem aktuellen Stand.
- Bestellung eines Datenschutzbeauftragten (TÜV-zertifiziert).
- Bestellung einer Informationssicherheitsbeauftragten (TÜV-zertifiziert).
- Einbindung von DSB und ISB in Datenschutzfolgenabschätzungen und Compliance Committee.
- Regelmäßige datenschutzrechtliche Schulung von Mitarbeitern.
- Verpflichtung der Mitarbeiter auf Vertraulichkeit beim Umgang mit personenbezogenen Daten.
- Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis.

b) Incident-Response-Management / Störungsfall-Management

*Prozess, wie auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen reagiert wird sowie hierzu vorbeugende Maßnahmen und Prozesse.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Prozess zum Umgang mit Störfällen und zur Einhaltung von Meldefristen gegenüber Betroffenen und Aufsichtsbehörden.

c) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Beachtung des Prinzips Datenschutz durch Technikgestaltung („privacy-by-design“).
- Beachtung des Prinzips Datenschutz durch datenschutzfreundliche Voreinstellungen („privacy-by-default“).

d) Auftragskontrolle / Einbindung von Unter-Auftragsverarbeitern

*Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, bspw. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl von Dienstleistern, Vorabüberzeugungspflicht, Nachkontrollen.*

Vom Auftragnehmer wurden folgende technische und organisatorische Maßnahmen umgesetzt:

- Sorgfältige Auswahl der (Unter-)Auftragsverarbeiter hinsichtlich umgesetzter technischer und organisatorischer Maßnahmen (TOMs) und Gewährleistung geeigneter Garantien.
- Vorherige und regelmäßige – zumindest stichprobenartige – Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten in Bezug auf die umgesetzten TOMs und auf den vertraglich verankerten Verarbeitungszweck.
- Formale Auftragserteilung inkl. vertragliche Vereinbarung zur Auftragsverarbeitung.
- Dokumentation der Leistungen und Pflichten von Auftragnehmer / Auftragsverarbeiter und Auftraggeber / Verantwortlicher.
- Wirksame Kontrollrechte sind vereinbart.
- Alle Weisungen sind schriftlich dokumentiert.
- Auftragsverarbeiter hat erforderlichenfalls Datenschutzbeauftragten bestellt.
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf Vertraulichkeit bzw. Datengeheimnis und Fernmeldegeheimnis.
- Sicherstellung der Rückgabe und / oder Vernichtung von Daten nach Beendigung des Auftrags.

1.5 Dokumentation (Art. 32 Abs. 1 lit. der DSGVO; Art. 25 Abs. 1 DSGVO)

- Leitlinie zu Informationssicherheit und Datenschutz (MMLL-4600).
- Interne Verhaltensregeln (bspw. Verpflichtungserklärungen und Verhaltenskodex)
- Weitere Handbücher, Richtlinien/Verhaltensregeln, Verfahrens- und Arbeitsanweisungen, Prozessdokumentationen, Funktions- und Tätigkeitsbeschreibungen, Risikoanalysen und -bewertungen und weitere einschlägige Steuerungs- und Nachweisdokumente im Rahmen des TÜV-zertifizierten Multi-Management Systems.

1.6 Zertifizierungen / Attestierungen

- DIN EN ISO 9001:2015
- DIN EN ISO 14001:2015
- DIN EN ISO/IEC 27001:2017
- ISAE-3402 / SOC-2

**2. Datenschutzbeauftragte**

2.1. Auftragnehmer

| | |
|---|---|
| Name, Vorname | **Haßkerl, Kilian** |
| Telefon | +49 6021 5001-316 |
| E-Mail | data.protection@asc.de |

2.2. Auftraggeber

| | |
|---|---|
| Name, Vorname<br>Telefon<br>E-Mail | |
| Bei externer Bestellung folgende Zusatzangaben:<br>Firma<br>Straße<br>PLZ Ort<br>Land | |
| ☐ Ein Datenschutzbeauftragter ist nicht bestellt, da die gesetzlichen Voraussetzungen für eine Bestellung nicht vorliegen. | |

2.3. Zuständige Aufsichtsbehörde

| | |
|---|---|
| Bezeichnung | **Bayerisches Landesamt für Datenschutzaufsicht** |
| Hausanschrift | Promenade 18, DE 91522 Ansbach |
| Postanschrift | Postfach 1349, DE 91504 Ansbach |
| Land | Deutschland |
| Telefon / Telefax | +49 981 180093-0 / +49 981 180093-800 |
| E-Mail | poststelle@lda.bayern.de |

**3. Weisungsempfänger und Weisungsberechtigte**

3.1 Auftragnehmer

| | |
|---|---|
| Name, Vorname | **Fengler, Tobias** |
| Funktion | Chief Engineering Officer |
| Telefon | +49 6021 5001-355 |
| E-Mail | t.fengler@asc.de |
| Weisungsbereich | Engineering / Service |
| Name, Vorname | **Bieder, Katja** |
| Funktion | Leiterin Service Administration |
| Telefon | +49 6021 5001-246 |
| E-Mail | k.bieder@asc.de |
| Weisungsbereich | Engineering / Service |

3.2. Auftraggeber

| | |
|---|---|
| Name, Vorname | |
| Funktion | |
| Telefon | |
| E-Mail | |
| Weisungsbereich | |
| Name, Vorname | |
| Funktion | |
| Telefon | |
| E-Mail | |
| Weisungsbereich | |

**4. Unterauftragsverarbeiter**

4.1 Externe

| | |
|---|---|
| Firmenname | **Microsoft Deutschland GmbH**, Walter-Gropius-Strasse 5, 80807 München, Deutschland |
| Auftragsbestandteil | ▪ Microsoft Office 365: Büroanwendungen (E-Mail, Kalender, Kontakte, Textverarbeitung, Tabellenkalkulation, OneDrive, SharePoint, Teams, usw.).<br>▪ Microsoft Dynamics 365: Customer Relationship Management.<br>▪ Microsoft Azure: Azure Active Directory & Azure Domain Managed Services, diverse virtuelle Server (IAAS, Azure Web Application Proxy).<br>Microsoft betreibt die vorstehenden Dienste aus der Cloud, hostet die entsprechenden Daten und gibt umfangreiche nachstehende Sicherheitsgarantien, die ASC lediglich weitergeben kann:<br>▪ https://privacy.microsoft.com/de-de/privacystatement/<br>▪ https://servicetrust.microsoft.com/<br>▪ https://azure.microsoft.com/de-de/support/legal/<br>https://www.microsoft.com/en-us/trust-center/product-overview/ |
| Firmenname | **EML European Media Laboratory GmbH** |
| Straße | Berliner Straße 45 (Mathematikon) |
| PLZ Ort | DE 69120 Heidelberg |
| Land | Deutschland |
| Telefon | +49 6221 533 323 |
| E-Mail | anja.varga@eml.com |
| Auftragsbestandteil | Entwicklungsleistung und technische Unterstützung (3rd Level Support) für Keyword Spotting / Transcription |

4.2 Interne (verbundene Konzernunternehmen, die sich in Mehrheitsbesitz und unter Kontrolle des Auftragnehmers befinden)

| | |
|---|---|
| Firmenname | **ASC Technologies GmbH** |
| Straße | Nell-Breuning-Allee 6 |
| PLZ Ort | DE 66115 Saarbrücken |
| Land | Deutschland |
| Telefon | +49 681 844968-0 |
| E-Mail | saarbruecken@asctechnologies.com |
| Auftragsbestandteil | Softwareentwicklung und technische Unterstützung (2nd / 3rd Level Support) |
| Firmenname | **ASC Cloud Solutions SRL** |
| Straße | Bulevardul MUNCII Nr. 22 A birou 2.1; Etaj 2 |
| PLZ Ort | RO 500281 Brasov |
| Land | Rumänien |
| Telefon | +40 751 299797 |
| E-Mail | brasov@asctechnologies.com |
| Auftragsbestandteil | Softwareentwicklung und technische Unterstützung (2nd / 3rd Level Support) |
| Company name | **ASC Technologies S.R.L.** |
| Street | Via Privata Santi Nabore e Felice 7 |
| ZIP code Place. | MI 20147 Milano |
| Country | Italy |
| Phone | +39 02 4802 7177 |
| E-mail | italy@asctechnologies.com |
| Scope of order | Softwareentwicklung und technische Unterstützung (2nd / 3rd Level Support) |

**In Ergänzung dieser Vereinbarung zur Auftragsverarbeitung gilt:**

- Es bestehen keine Sondervereinbarungen -