Vertrag zur Auftragsverarbeitung (gemäß Art. 28 DS-GVO)

Vereinbarung
zwischen der

Firma
Straße und Hausnummer

PLZ und Ort

- nachstehend Auftraggeber genannt -
und der

aConTech Enterprise IT-Solutions GmbH
Mohnweg 9
90768 Fürth

- nachstehend Auftragnehmer genannt -

Inhaltsverzeichnis

1. Gegenstand und Dauer des Auftrags 3
   1.1. Gegenstand des Auftrags 3
   1.2. Dauer des Auftrags 4
2. Konkretisierung des Auftragsinhalts 4
   2.1. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten 4
   2.2. Art der Daten 5
   2.3. Kreis der Betroffenen 5
   2.4. Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO): 5
   2.5. Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO) 6
3. Berichtigung, Sperrung und Löschung von Daten 7
4. Pflichten des Auftragnehmers 7
5. Pflichten des Auftraggebers 11
6. Unterauftragsverhältnisse (Subunternehmer) 11
8. Rechte und Pflichten, sowie Weisungsbefugnis des Auftraggebers 13
9. Löschung von Daten und Rückgabe von Datenträgern 15
10. Schlussbestimmung 16

Anlage 1 – Technisch-organisatorische Maßnahmen 17
   1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 17
   2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO) 17
   3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) 17
   4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) 17

Anlage 2: Genehmigte Subunternehmer 18

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand des Auftrags

Der Gegenstand des Auftrags umfasst folgendes (bitte auswählen und ergänzen):

☐ Consulting, Umsetzung, Implementierung, Betrieb und Wartung von Lösungen zu Microsoft Office 365, Microsoft Azure, sonstigen Cloud-Diensten oder lokaler IT-Infrastruktur
☐ Consulting zur IT- oder Unternehmensstrategie und Prozessen
☐ Bereitstellung von (Cloud) Lizenzen und Betrieb von Cloud-Services laut der „AGB Cloud aConTech CSP"
☐ Bereitstellung von Software-Ressourcen (auch durch Unterauftragnehmer gemäß ADV)
☐ Administration, Migration, Implementierung und Ausbau von IT-Systemen des Auftraggebers mit der Möglichkeit des Zugriffs auf personenbezogene Daten
☐ Operative Verarbeitung personenbezogener Daten im Rahmen der Leistungserbringung (z.B. aConTech Managed Services)
☐ Detaillierte Beschreibung des Gegenstands im Hauptauftrag Hauptauftragsname vom Datum
☐ Weiteren Gegenstand des Auftrags einfügen.
☐ Weiteren Gegenstand des Auftrags einfügen.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. 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 der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

1.2. Dauer des Auftrags

Der Vertrag wird auf unbestimmte Zeit geschlossen. Die Laufzeit und Kündigung dieses Vertrages richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages. Eine Kündigung des Hauptvertrages bewirkt automatisch auch eine Kündigung dieses Vertrags. Falls kein Hauptvertrag existiert, beträgt die Kündigungsfrist vier Wochen zum Monatsende.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Konkretisierung des Auftragsinhalts

2.1. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

Der Auftragnehmer erhebt, verarbeitet und nutzt die personenbezogenen Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers. Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle.

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden. Der Zweck, der Umfang und die Art sind wie folgt (gemäß der Definition von Art. 4 Nr. 2 DSGVO):

☒ „1.1 Gegenstand des Auftrags“ dieses Vertrags
☒ Bereitstellung von Cloud-Services und Lizenzen laut der „AGB Cloud aConTech CSP“
☐ Zweck, Umfang und Art der Verarbeitung ergeben sich aus dem Hauptvertrag bzw. aus der Leistungsbeschreibung vom Für Datum klicken

2.2. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien):

- ☒ 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)
- ☐ Ggf. weitere Art einfügen.
- ☐ Ggf. weitere Art einfügen.

2.3. Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- ☒ Beschäftigte i. S. d. § 3 Abs. 11 BDSG
- ☒ Kunden
- ☒ Partner
- ☒ Lieferanten
- ☐ Ggf. weitere Betroffene einfügen
- ☐ Ggf. weitere Betroffene einfügen

2.4. Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- ☒ Personenstammdaten, Identifikationsdaten, ommunikations-daten, Bemerkungen/Nachrichten
- ☒ Adressdaten (Adresse, Telefonnummer, E-Mail)
- ☒ Kommunikationsdaten
- ☒ Elektronische Identifikationsdaten
- ☐ Gesundheitsdaten
- ☐ Steuerdaten
- ☐ Sozialversicherungsdaten
- ☐ Bemerkungen, Nachrichten
- ☐ Ggf. weitere Kategorie einfügen.
- ☐ Ggf. weitere Kategorie einfügen.
- ☐ Ggf. weitere Kategorie einfügen.

2.5. Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

(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 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
(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.

Das in Anlage 1 beschriebene Datenschutzkonzept stellt die Mindestanforderungen der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar. Hierbei ist auch das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung beschrieben.

Der Auftragnehmer hat bei gegebenem Anlass oder auch auf Aufforderung des Auftraggebers eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen. Bei der Aufforderung durch den Auftraggeber teilt der Auftragnehmer dem Auftraggeber vor Beginn des Audits die voraussichtlichen Kosten mit.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

3. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
Sollte ein Betroffener seine Rechte auf Berichtigung, Löschung oder Sperrung von personenbezogenen Daten oder auf Auskunft über die gespeicherten personenbezogenen Daten, den Zweck der Speicherung und die Personen und Orte, an die personenbezogenen Daten regelmäßig übermittelt werden, geltend machen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann.
Der Auftragnehmer wird personenbezogene Daten des Auftraggebers nicht gegenüber Strafverfolgungsbehörden offenlegen, sofern nicht gesetzlich vorgeschrieben. Sollte sich eine Vollstreckungsbehörde mit dem Auftragnehmer oder Microsoft in Verbindung setzen und personenbezogene Daten anfordern, versucht der Auftragnehmer sowie Microsoft, die Vollstreckungsbehörde an den Auftraggeber zu verweisen, damit sie diese Daten direkt beim Auftraggeber anfordert. Wenn der Auftragnehmer, Subunternehmer oder Microsoft verpflichtet sind, personenbezogene Daten gegenüber einer Vollstreckungsbehörde offenzulegen, wird der Auftragnehmer und Microsoft den Auftraggeber unverzüglich darüber informieren und ihm eine Kopie der Aufforderung zukommen lassen, sofern dies nicht gesetzlich verboten ist.

4. Pflichten des Auftragnehmers

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 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

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

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

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den definierten Weisungsempfänger des Auftragnehmers weiterzuleiten.

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 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

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 erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.
Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

- ☐ Bankgeheimnis
- ☐ Fernmeldegeheimnis
- ☐ Sozialgeheimnis
- ☐ Berufsgeheimnisse nach § 203 StGB
- ☐ Ggf. weitere Geheimnisschutzregel
- ☐ Ggf. weitere Geheimnisschutzregel

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
Dessen Kontaktdaten lauten:

René Rautenberg GmbH
René Rautenberg
Jägerwirtstraße 3
81373 München
Tel.: 089/552 94 87 0
Fax: 089/552 94 87 9
Mail: datenschutzbeauftragter@acontech.de

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, 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.

c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

e. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g. 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.

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

5. Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

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

6. Unterauftragsverhältnisse (Subunternehmer)

Die zukünftige Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer ohne gesonderte Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. Der Auftragnehmer muss dafür

Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).
Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage 2 – Unterauftragsverhältnisse mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben, sofern die bisher vereinbarten und von Auftragsverarbeiter zugesicherten technischen und organisatorischen Maßnahmen nicht vollständig gewährleistet werden können (§ 28 Abs. 2 Satz 2 DS-GVO). In diesem Fall darf die beabsichtigte Änderung nicht vollzogen werden.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

8. Rechte und Pflichten, sowie Weisungsbefugnis des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22

DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
Der Auftraggeber ist berechtigt, sich wie unter Nr. 4 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

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

Weisungsberechtigte Funktionen des Auftraggebers sind:

Name und Kontaktdaten von weisungsberechtigten Funktionen

Weisungsempfänger beim Auftragsverarbeiter sind: Der jeweilige für den konkreten Auftrag verantwortliche Mitarbeiter des Auftragsverarbeiters Für Weisung zu nutzende Kommunikationskanäle:

- Per E-Mail an die persönliche Mailadresse des Ansprechpartners (Account-Manager, Consultant, etc.) oder support@acontech.de
- Per Telefon an die persönliche Telefonnummer des Ansprechpartners (Account-Manager, Consultant, etc.) oder +49 131314-60 (für Premium Support Kunden)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren

9. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. 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. Microsoft bewahrt seinerseits im Onlinedienst gespeicherte Kundendaten für die Dauer von 90 Tagen nach Ablauf oder Kündigung des Kundenabonnements in einem Konto mit eingeschränkter Funktionalität auf, damit der Kunde die Daten extrahieren kann. Nach Ablauf des Aufbewahrungszeitraums von 90 Tagen wird Microsoft das Konto des Kunden deaktivieren und die Kundendaten löschen. Der Onlinedienst unterstützt die Aufbewahrung und Extrahierung von Software, die der Kunde bereitgestellt hat, möglicherweise nicht. Microsoft haftet nicht für die Löschung von Kundendaten wie in diesem Abschnitt beschrieben.

10. Schlussbestimmung

Änderungen, Ergänzungen und die Aufhebung dieses Vertrages bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelungen eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelungen am nächsten kommt und den Anforderungen der DS-GVO am besten gerecht wird. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand ist derjenige beim Auftragnehmer.

Auftragnehmer

Fürth, _____
Ort, Datum

_____ _____
Stefan Zenkel, Geschäftsführung Unterschrift

Auftraggeber

_____
Ort, Datum

_____ _____
Name, Funktion Unterschrift

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**, **Zugangskontrolle**, **Zugriffskontrolle**, **Trennungskontrolle, Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Maßnahmen werden durch das aConTech IT-Sicherheitskonzept beschrieben und umgesetzt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Die Maßnahmen werden durch das aConTech IT-Sicherheitskonzept beschrieben und umgesetzt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Die Maßnahmen werden durch das aConTech IT-Sicherheitskonzept beschrieben und umgesetzt.

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

aConTech arbeitet mit folgenden Maßnahmen:

- Datenschutz-Management auf Basis des ER Secure Management Systems mit jährlichen Audits und andauernder Maßnahmenüberprüfung und Entwicklung;
- Incident-Response-Management (IT-Störungsmanagement), siehe IT-Sicherheitskonzept;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- aConTech Notfallplan;
- Durchgängiger Melde- und Bearbeitungsprozess zur Wahrung von Betroffenenrechte und Datenschutzverstäößen
- Auftragskontrolle, siehe IT-Sicherheitskonzept

Das derzeit gültige IT-Sicherheitskonzept kann unter www.acontech.de/datenschutz eingesehen und heruntergeladen werden.

Anlage 2: Genehmigte Subunternehmer

Nr.	Unterauftragnehmer (Firma, Anschrift, Ansprechpartner)	Verarbeitete Datenkategorien	Verarbeitungsschritte / Zweck der Unterauftragsdatenverarbeitung
01	Microsoft Ireland Operations Ltd. Building 3, Carmanhall Road Sandyford Industrial Estate 18 Dublin, Ireland	Die Datenkategorien sind jeweils in Punkt 2 „Konkretisierung des Auftragsinhaltes“ zu finden.	Die Zurverfügungstellung und Erbringung von Wartungsleistungen der Microsoft Cloud Plattform und Dienste, sowie ggf. 3rd Level Support.
02	Microsoft Corporation One Microsoft Way Redmond, WA 98052, USA	Die Datenkategorien sind jeweils in Punkt 2 „Konkretisierung des Auftragsinhaltes“ zu finden.	Die Erbringung von möglichen Wartungsarbeiten und Bereitstellung an der Microsoft Cloud Plattform und Dienste, sowie ggf. 3rd Level Support.
03	ALSO Deutschland GmbH Lange Wende 43 59494 Soest	Die Datenkategorien sind jeweils in Punkt 2 „Konkretisierung des Auftragsinhaltes“ zu finden.	Bereitstellung des aConTech Kundenportals zur Verwaltung und Bereitstellung von Microsoft Online-Diensten, sowie ggf. 3rd Level Support.
04	Crayon Deutschland GmbH	Bajuwarenring 1, 82041 Oberhaching	Bereitstellung des aConTech Kundenportals zur Verwaltung und Bereitstellung von Microsoft Online-Diensten, sowie ggf. 3rd Level Support.
05	ADN Distribution GmbH	Josef-Haumann-Str. 10, 44866 Bochum	Bereitstellung des aConTech Kundenportals zur Verwaltung und Bereitstellung von Microsoft Online-Diensten, sowie ggf. 3rd Level Support.

aConTech GmbH
Mohnweg 9, 90768 Fürth
Zentrale: +49 911 131314-50
Fax: +49 911 131314-51
E-Mail: info@acontech.de

Geschäftsführer:
Stefan Zenkel
Amtsgericht Fürth
HRB 12 868
UST-IdNr. DE276326941

VR meine Bank eG
Konto: 11 32 393
BLZ: 760 695 59
IBAN: DE 21 7606 9559 0001 1323 93
BIC: GENODEF1NEA