Datenschutzrechtliche Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gemäß Art. 28 DS-GVO)

zwischen

- „Auftraggeber“ -

und

abtis GmbH
Wilhelm-Becker-Straße 11b
75179 Pforzheim
- „Auftragsverarbeiter“ -

1. Gegenstand und Dauer der Vereinbarung
Der Auftrag umfasst Folgendes:

- ☐ Administrative Wartung und Betreuung der beim Auftraggeber installierten IT-Infrastruktur
- ☐ Administrative Wartung und Betreuung der beim Auftraggeber genutzten Endgeräte
- ☐ Wartung oder Support eines Datenverarbeitungsverfahrens oder einer Datenverarbeitungsanlage mit der Möglichkeit des Zugriffs auf personenbezogene Daten, z.B. Monitoring von Kundensystemen, Security as a Service,
- ☐ Operative Verarbeitung personenbezogener Daten im Rahmen der Leistungserbringung, z.B. Managed E-Mail, Managed Services, Backup as a Service, Rechenzentrumsbetrieb
- ☐ Migration und Implementierung von Services und Anwendungen
- ☐ Sonstiges:

Der Auftragsverarbeiter 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).

Dauer des Auftrags:
Der Vertrag wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist 4 Wochen.
Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die

Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter 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. Zweck, Umfang und Art der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

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 DS-GVO):

☐ Zweck, Umfang und Art der Verarbeitung ergeben sich aus dem Hauptvertrag bzw. aus der Leistungsbeschreibung vom

Alternativ

☐ Administrative Wartung, Betreuung und Support der Anwendungen des Auftraggebers.

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

☒ Beschäftigtendaten
☒ Interessenten- / Kundendaten
☒ Dienstleister- / Lieferantendaten
☐ Hier ggf. weitere betroffene Personen spezifizieren
☐ Hier ggf. weitere betroffene Personen spezifizieren

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

☒ Name, Vorname,
☒ Adresse
☒ Telefonnummer
☒ Email-Adresse
☐ Kontodaten
☐ Steuerdaten
☐ Sozialversicherungsdaten
☐ Kommunikationsdaten (z.B. zu Email, Internet, Telefon)
☐ Vertragsstammdaten
☐ Vertragsbewegungsdaten (z.B. Abrechnungsdaten und Zahlungsdaten
☐ Hier ggf. weitere Kategorien von personenbezogenen Daten eintragen
☐ Hier ggf. weitere Kategorien von personenbezogenen Daten eintragen

Besondere Kategorien von personenbezogenen Daten (entsprechend der Definition von Art. 9 und 10 DS-GVO):

☐ rassische und ethnische Herkunft
☐ politische Meinung
☐ religiöse oder weltanschauliche Überzeugung
☐ Gewerkschaftszugehörigkeit
☐ genetische Daten
☐ biometrische Daten
☐ Gesundheitsdaten
☐ Daten zum Sexualleben oder zur sexuellen Orientierung
☐ Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln
☐ Hier ggf. weitere besondere Kategorien von personenbezogenen Daten eintragen

3. Rechte und Pflichten sowie Weisungsbefugnisse 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 Auftragsverarbeiter 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 Auftragsverarbeiter 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 Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Hierzu stellt der Auftragsverarbeiter alle notwendigen Unterlagen in Textform zur Verfügung. Der Auftragsverarbeiter kann für darüber hinausgehende Prüfungen des Auftraggebers (Vor Ort Prüfungen) die ihm entstandenen Kosten geltend machen.
Der Auftraggeber informiert den Auftragsverarbeiter 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 Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragsverarbeiters
Weisungsberechtigte Funktionen des Auftraggebers sind:

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

☒ per Email an folgende Adresse: Email-Adresse des Ansprechpartners
oder support@abtis.de
☒ per Telefon an folgende Rufnummer: Support-Hotline: +49 721 4431 200

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.

5. Pflichten des Auftragsverarbeiters
Der Auftragsverarbeiter 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/Auftraggeber 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 Auftragsverarbeiter 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 Auftragsverarbeiter 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.
Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

☒ Verfügbarkeitskontrolle der Daten durch mindestens tägliche Datensicherung, sofern die Auftragsverarbeitung auf Systemen im Verfügungsbereich des Auftragsverarbeiters erfolgt
☒ Plausibilitätskontrolle der Verarbeitungsergebnisse
☐

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 Auftragsverarbeiter 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 folgende Stelle des Auftraggebers weiterzuleiten:

☒ Die in Ziffer 4 genannte weisungsberechtigte Funktion
☐ an die folgende Person oder Funktion:

Der Auftragsverarbeiter 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 Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
Der Auftragsverarbeiter 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 Auftragsverarbeiters dem nicht entgegenstehen.
Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
Der Auftragsverarbeiter 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 erforder-

lichen 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 Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit/Home Office von Beschäftigten des Auftragsverarbeiters) ist nur mit Zustimmung des Auftraggebers 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 Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutz-rechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

☐ Bankgeheimnis
☐ Fernmeldegeheimnis nach dem TKG und TMG
☐ Sozialgeheimnis
☐ Berufsgeheimnis nach § 203 StGB
☐ Sonstiges:

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personen-bezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Da-tenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Be-schäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragsverarbeiter überwacht die Einhaltung der da-tenschutzrechtlichen Vorschriften in seinem Betrieb.

☒ Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz bestellt:
Name, Vorname: Zlamal Ralf
Organisationseinheit: IITR Datenschutz Regionalpartner Baden-Württemberg
Kontaktdaten: 089/18917360 - zlamal@iitr.de
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen

6. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters 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 Auftragsverarbeiter 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 Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern für Kerndienstleistungen (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die zukünftige Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragsverarbeiter **ohne gesonderte Genehmigung** des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. Der Auftragsverarbeiter 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 vor einer Auftragsvergabe. Der Auftraggeber kann aus wichtigem Grund der Beauftragung widersprechen.

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 Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters 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 Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

- ☒ Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre) mittels eines Fragenkataloges (sofern dies möglich ist) oder alternativ anhand der Datenschutzerklärung des jeweiligen Subunternehmers
- ☒ Regelmäßige Prüfung des beim Subunternehmer eingerichteten Datenschutzkonzeptes (mindestens alle 2 Jahre) (sofern dies möglich ist)
- ☐ Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre) durch eine Begehung vor Ort.
- ☐ Regelmäßige Einholung von Zertifikaten über eine gültige Zertifizierung nach der DS-GVO.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.
Der Auftragsverarbeiter haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
Zurzeit sind für den Auftragsverarbeiter
☒ die in der Anlage 1 dokumentierten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt.
Mit der Beauftragung der in Anlage 1 genannten Subunternehmer 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. Der Auftraggeber erhält die Möglichkeit, 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.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung 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 DS-GVO, 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 Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene und nachvollziehbare Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen berücksichtigt.

Das in Anlage 2 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.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:
☐ Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragsverarbeiters wurden am
durch folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Regelungen nach Art. 42:

Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

Oder:

☒ Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, 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.
Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragsverarbeiter und Auftraggeber abzustimmen.
Soweit die beim Auftragsverarbeiter getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.
Die Maßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
Wesentliche Änderungen muss der Auftragsverarbeiter mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

☐ dem Auftraggeber auszuhändigen.

oder

☐ wie nachfolgend beschrieben datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

☐ Löschung unter Zuhilfenahme eines für die sichere Datenlöschung zugelassenen Softwareprogramms

☐ Löschung durch mehrmaliges (mind. 3 faches) Überschreiben des Datenträgers mit Ziffern und Zeichen

☐ Vernichtung durch ein auf die Vernichtung von Datenträger spezialisiertes Unternehmen

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das für den Auftraggeber örtlich zuständige Gericht vereinbart.
Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter 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 Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Für den Auftraggeber:	Für den Auftragsverarbeiter:
Name:	Name: Thorsten Weimann
Position:	Position: Geschäftsführer
Unterschrift: _____	Unterschrift: ohne separate Unterschrift gültig

Anlage 1 - Unterauftragsverhältnisse

Aktuell bestehen die nachfolgenden Unterauftragsverhältnisse im Zusammenhang mit der Auftragsverarbeitung:

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA
Datenschutzerklärung:
https://privacy.microsoft.com/de-de/privacystatement

Barracuda Networks, Inc.
(US) Corporate Headquarters
3175 Winchester Blvd
Campbell, California 95008
United States
Datenschutzerklärung:
https://de.barracuda.com/company/legal/trust-center/data-privacy/privacy-policy

Anlage 2 – Technische und organisatorische Maßnahmen / Datenschutzkonzept

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DS-GVO und ggf. weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DS-GVO.
Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Die Räume, in denen die Verarbeitung personenbezogener Daten erfolgt oder Datenverarbeitungsanlagen installiert sind, sind nicht frei zugänglich. Sie sind bei Abwesenheit der Mitarbeiter verschlossen. Die Zutrittsberechtigungen sind in einem geregelten Verfahren nach dem „need to know Prinzip“ vergeben und werden regelmäßig hinsichtlich ihrer Erforderlichkeit überwacht. Räume, in denen Datenverarbeitungsanlagen (Rechenzentrum, Server, Netzwerkverteiler usw.) untergebracht sind, sind besonders zutrittsgeschützt und sind nur für Beschäftigte der IT-Administration und ggfs. der Geschäftsleitung) zugänglich. Alternativ sind die Geräte in geeigneten und verschlossenen Schränken untergebracht. Besucher und unternehmensfremde Personen werden in einem dokumentierten Verfahren registriert und innerhalb der Geschäftsräume beaufsichtigt.

1.2. Zugangskontrolle

Für jeden Netzwerkbenutzer ist ein persönlich zugeordneter Benutzer mit einem mindestens 9-stelligen Passwort mit Groß- und Kleinbuchstaben, Ziffer und Sonderzeichen eingerichtet. Die Nutzeranmeldung erfolgt zusätzlich mittels Multifaktorauthentifizierung. Die Netzwerkbenutzer sind auf die Einhaltung der Benutzerzugangsrichtlinie dokumentiert verpflichtet. Die Einrichtung, Änderung und der Entzug von Zugangsberechtigungen erfolgt in einen dokumentierten Verfahren. Eingerichtete Zugangsberechtigungen werden regelmäßig hinsichtlich ihrer Erforderlichkeit dokumentiert überprüft. Die Netzwerkzugriffe werden überwacht und protokolliert, dies beinhaltet auch nicht erfolgreiche Anmeldeversuche. Ein Netzwerkzugang wird automatisiert nach spätestens 10 Fehlversuchen systemseitig gesperrt.

1.3 Zugriffskontrolle

Für die Zugriffe auf personenbezogene Daten ist ein dokumentiertes, rollenbasiertes Berechtigungskonzept vorhanden, welches die Zugriffe in der Form einschränkt, dass nur berechtigte Personen auf die für ihre Aufgabe notwendigen personenbezogenen Daten zugreifen können (Minimumprinzip). Die Passwort-Regelungen aus der Zugangskontrolle werden auch im Rahmen der Zugriffskontrolle umgesetzt. Die administrativen Tätigkeiten sind auf einen kleinen Kreis von Administratoren eingeschränkt. Die Tätigkeiten der Administratoren werden im Rahmen technisch vertretbaren Aufwandes überwacht und protokolliert.

1.4 Pseudonymisierung
Auswertungen werden pseudonymisiert, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.

1.5 Trennungskontrolle
Die Trennung von personenbezogenen Daten wird durch unterschiedliche Speicherorte oder durch eine Mandantentrennung sichergestellt.

2. Integrität
2.1 Weitergabekontrolle
Im Rahmen der Weitergabekontrolle wird sichergestellt, dass nur berechtigte Personen die personenbezogenen Daten zur Kenntnis nehmen können. Bei einer Übermittlung per E-Mail sind entsprechende Schutzmaßnahmen (z.B. Verschlüsselung der Kommunikation zwischen den Mail-Servern) eingerichtet. Mobile Geräte oder mobile Speichermedien werden verschlüsselt werden, wenn auf ihnen personenbezogene Daten gespeichert werden.

2.2 Eingabekontrolle
Die Eingabe, Änderung und Löschung personenbezogener Daten kann dem durchführenden Beschäftigten zugeordnet werden. Die Änderung und Löschungen von Datensätzen ist systemseitig eingeschränkt, damit ein versehentliches Ändern oder Löschen wirksam verhindert wird.

2.3 Auftragskontrolle
Im Rahmen der Auftragskontrolle wird sichergestellt, dass die im Auftrag durchgeführten Datenverarbeitungsvorgänge ausschließlich auf Weisung des Auftraggebers erfolgen. Hierzu werden die mit der Datenverarbeitung Beschäftigten geschult und unterwiesen. Die Auftragsverarbeitung wird durch interne Kontrollen überwacht. Die Ergebnisse der Kontrollen werden dokumentiert.
Unterauftragnehmer werden nur auf Basis der mit dem Auftraggeber vereinbarten Regelungen beauftragt. Die Übermittlung oder der Zugriff auf personenbezogene Daten erfolgt erst dann, wenn der Unterauftragnehmer eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO unterzeichnet hat und die Einhaltung der Regelungen des Datenschutzkonzeptes bestätigt hat. Die Prüfpflicht des Auftragnehmers gegenüber seinem Unterauftragnehmer ergibt sich aus der mit dem Auftraggeber abgeschlossenen Vereinbarung zur Auftragsverarbeitung.

3. Verfügbarkeit und Belastbarkeit
Die Verarbeitung von personenbezogenen Daten erfolgt auf Datenverarbeitungssystemen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen. Es sind keine Systeme im Netz verbunden, die außerhalb der Wartungszyklen der Hersteller sind (insb. kein Windows XP, Windows Server 2003 etc.). Sicherheitsrelevante Patches werden innerhalb von 72 Stunden nach Bekanntgabe eingespielt, sofern keine weiteren Risiken für den Systembetrieb bestehen. Die durchgängige Verfügbarkeit von personenbezogenen Daten wird mittels redundanten Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet. Rechenzentren und Serverräume entsprechen dem Stand der Technik (Temperaturregelung, Brandschutz, Wassereinbruch etc.). Die Server verfügen über eine unterbrechungsfreie

Stromversorgung (USV), die im Notfall ein geregeltes Herunterfahren ohne Datenverlust sicherstellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es ist ein Verfahren zur Überwachung des Datenschutzes im Unternehmen implementiert. Dieses beinhaltet die Verpflichtung der Beschäftigten auf das Datengeheimnis, die Schulung und Sensibilisierung der Beschäftigten und die regemäßige Auditierung der Datenverarbeitungsverfahren. Ebenso ist die Dokumentation des für den Auftraggeber durchgeführten Verarbeitungsverfahrens sichergestellt. Für Datenschutzverletzungen und die Wahrung der Betroffenenrechte ist ein durchgängiger Meldeprozess und Bearbeitungsprozess eingeführt. Dieser beinhaltet auch die Information des Auftraggebers.