Anlage 4 - Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Präambel

Zwischen der

- nachfolgend Auftraggeber genannt -

und der

abilis GmbH

- nachfolgend Auftragnehmer genannt -

Präambel

Der Auftragnehmer ist ein IT-Komplettdienstleister für den klassischen Mittelstand und bedient die gesamte Wertschöpfungskette - von der Beratung über die Einführung bis hin zum Betrieb der Lösungen im eigenen Green IT-Hochleistungsrechenzentrum.

Hierbei

- verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers, oder
- kann nicht ausschließen, dass er Zugriff auf oder Kenntnis von personenbezogenen Daten des Auftraggebers erlangt.

Daher hat der Auftraggeber im Rahmen seiner Sorgfaltspflichten und unter Berücksichtigung der Datenschutzgrundverordnung (DSGVO) den Auftragnehmer als Dienstleister ausgewählt. Erforderlich ist, dass die Parteien die besonderen Rechte und Pflichten zum Datenschutz gesondert in einem speziellen Vertrag (sog. Auftragsverarbeitungsvertrag) regeln. Hierzu dient dieser Vertrag.

1 Allgemeines

1.1 Zwischen den Vertragsparteien besteht ein Vertragsverhältnis, bei dem der Auftragnehmer entweder personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) verarbeitet oder die Möglichkeit der Kenntnisnahme von personenbezogenen Daten des Auftraggebers hat. Voraussetzung hierfür ist gemäß Art. 28 Abs. 2 DSGVO (Datenschutzgrundverordnung) ein Auftragsverarbeitungsvertrag, mithin dieser Vertrag, der die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung regelt.

1.2 Dieser Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem o. g. Hauptvertrag im Zusammenhang stehen und bei denen Mitarbeiter, Vertreter oder Organe des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

2 Rechte und Pflichten des Auftragnehmers

2.1 Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu den personenbezogenen Daten hat, dürfen diese personenbezogenen Daten ausschließlich im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

2.2 Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer findet ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Falls ein Unterauftragnehmer beauftragt werden soll, gelten diese Anforderungen ebenfalls für diese.

2.3 Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

2.4 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung aller erforderlichen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 3 S. 2 lit.c i.V.m. Art. 32 DSGVO und diese Maßnahmen zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Die zu treffenden Maßnahmen müssen ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme erreichen. 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 zu berücksichtigen. Das Ergebnis ist zu dokumentieren (vgl. Art. 28 Abs. 3 lit. C, 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO). Diese Maßnahmen werden diesem Vertrag als Anlage 3 beigefügt. Da die technischen und rechtlichen Gegebenheiten Änderungen unterliegen, sind sich die Parteien bewusst, dass Änderungen an den Maßnahmen erforderlich sein können. Daher wird der Auftragnehmer die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren und anpassen. Dem Auftragnehmer ist es gestattet, alternative adäquate Maßnahmen umzusetzen. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

2.5 Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der Anlage 1 benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

2.6 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgeabschätzungen oder vorheriger Konsultationen), sowie bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Für diese Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten sind, kann der Auftragnehmer eine Vergütung beanspruchen.

2.7 Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden (Art. 28 Abs. 3 S. 2 lit.b, 29, 32 Abs. 4 DSGVO.

2.8 Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO bestellt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen. Dies Pflicht kann entfallen, der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

2.9 Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

2.10 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei dem Verdacht von Verstößen gegen datenschutzrechtliche Vorschriften oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des

Auftraggebers. Auch wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird, soweit sie sich auch auf diesen Auftrag beziehen.

2.11 Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

– eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

– eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

2.12 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 Personen gewährleistet wird.

2.13 Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

3 Rechte und Pflichten des Auftraggebers

3.1 Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung.

3.2 Der Auftraggeber hat jederzeit das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Der Auftraggeber erteilt alle Aufträge schriftlich oder per E-Mail. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail bestätigen.

3.3 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Erfüllung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

3.4 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.5 Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

3.6 Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen.

3.7 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durzuführen oder durch eine dritte Person durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Das Kontrollrecht kann nicht durch Dritte wahrgenommen werden und findet seine Grenze bei Betriebs- oder Geschäftsgeheimnissen des Auftragnehmers. Das Ergebnis der Kontrolle wird durch den Auftraggeber jeweils dokumentiert.

3.8 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

3.10 Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der Anlage 1 benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

4 Kontrollbefugnisse

4.1 Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

4.2 Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

4.3 Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

4.4 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

4.5 Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

5 Unterauftragsverhältnisse

5.1 Der Auftragnehmer darf nur nach vorheriger ausdrücklicher schriftlicher Zustimmung Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einsetzen. Alle schon zum Vertragsschluss bestehenden Unterauftragsverhältnisse sind in der Anlage 2 zu diesem Vertrag angegeben. Der Auftraggeber stimmt der Beauftragung dieser genannten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

5.2 Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unter-auftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information"). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der

„Information" zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information" erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

5.3 Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

5.4 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

5.5 Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

5.6 Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

5.7 Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

6 Geheimhaltungspflichten

6.1 Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

6.2 Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

7 Laufzeit, Kündigung

7.1 Der Vertrag läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

7.2 Der Auftraggeber kann diese Vereinbarung zur Auftragsdatenvereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

7.3 Unabhängig von den vorstehenden Regelungen zu den Laufzeiten gilt die Geheimhaltungspflicht und vereinbarte Aufbewahrungsfristen über das Vertragsende hinaus.

8 Schlussbestimmungen

8.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutzgrundverordnung liegen.

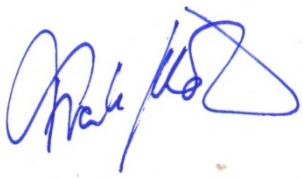
8.2 Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen

8.3 Für Nebenabreden ist die Schriftform erforderlich. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

8.4 Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____ _____

Ort, Datum Unterschrift des Auftraggebers



_____ _____

Ort, Datum Unterschrift des Auftragnehmers

Anlage 1 - Gegenstand des Auftrags

1. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: _____

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

☐ Stammdaten ☐ Adressdaten ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)

☐ Termindaten ☐ Abrechnungsdaten ☐ Vertragsdaten ☐ Bankverbindungsdaten

☐ Planungsdaten ☐ Kundenhistorie ☐ Auskunftsangaben (z.B. von Auskunfteien)

☐ Sensible Daten (z.B. Gesundheitsdaten, Religionszugehörigkeit)

☐ Sonstige: _____

2. Kategorien betroffener Person

☐ Mitarbeiter ☐ Kunden/Interessenten ☐ Abonnenten

☐ Handelsvertreter

☐ Rentner ☐ Angehörige ☐ Lieferanten/Dienstleister

☐ Kontaktpersonen ☐ Sonstige: _____

3. Weisungsberechtigte Personen des Auftraggebers

4. Weisungsempfangsberechtigte Personen des Auftragnehmers

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer"). Dabei handelt es sich um nachfolgende Unternehmen:

TelemaxX Telekommunikations GmbH

Amalienbadstrasse 41, Bau 61

D-76227 Karlsruhe

Die TelemaxX Telekommunikations GmbH stellte Rechenzentrumsfläche für die abilis GmbH zur Verfügung und verfügt über einen Datenschutzbeauftragten sowie Zertifizierungen nach DIN ISO 27001. Der Unterauftragnehmer wird regelmäßig vom Auftragnehmer auf seine Zuverlässigkeit geprüft.

b.i.g. sicherheitstechnik und logistik gmbh

Ehrmannstrasse 6

D-76135 Karlsruhe

Dienstleistungen: Gebäudesicherheit, Objektüberwachung und Zutrittskontrolle des Stammsitzes des Auftragnehmers in Stutensee.

Reißwolf Akten und Datenvernichtungs GmbH

Eisentalstraße 6

D-71332 Waiblingen

Datenvernichtung / Aktenvernichtung nach DIN

abilis IT
IT-Services & Consulting

Anlage 3 – Technische und organisatorische Maßnahmen (Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO)

Der Auftragnehmer erklärt, dass er unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Sicherheitsmaßnahmen getroffen hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftragnehmer hat ein Informationssicherheitsmanagementsystem (ISMS) auf Grundlage der ISO 27001:2013 im Unternehmen implementiert. Das ISMS ist ein integraler Bestandteil der technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten.

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

a. Der Auftragnehmer verwehrt Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen sie personenbezogene Daten verarbeitet mit folgenden Maßnahmen (Zutrittskontrolle)

aa. Der Hauptsitz des Auftraggebers befindet sich in einem alleine genutzten Geschäftshaus in der Lorenzstraße 8 in 76297 Stutensee. Diese **Räumlichkeiten** des Auftragnehmers sind gegen den unbefugten Zutritt wie folgt abgesichert:

- Die Außentüren sind mit Transponder-Schließsystem mit individualisierten Berechtigungen ausgestattet und grundsätzlich verschlossen;
- Das Gebäude ist mit einer Alarmanlage gesichert, welche von einer Sicherheitszentrale 24/7 überwacht wird; die Alarmanlage kann nur von einem fest definierten Personenkreis deaktiviert werden; der Zutritt außerhalb der Geschäftszeiten kann nur nach vorheriger Anmeldung bei der Sicherheitszentrale durch eine autorisierte Personen erfolgen; näheres ist in einem Verfahren geregelt.
- Alle Zugänge zum Haus sind videoüberwacht und werden aufgezeichnet.
- Das Personal, sowie Dritte (Reinigungs- und Wachpersonal) werden sorgfältig ausgewählt
- Besucher werden am Eingang kontrolliert und protokolliert; sie bewegen sich in den Räumlichkeiten, in denen personenbezogene Daten aufbewahrt werden, ausschließlich in Begleitung eines Mitarbeiters;
- Alle Gebäudeschächte sind durch bauliche Maßnahmen abgesichert;

bb. Darüber werden Systeme, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet werden, in einem am Unternehmenssitz betriebenen **Rechenzentrum** gespeichert, für welches folgende darüberhinausgehenden Maßnahmen getroffen wurden:

- Das Rechenzentrum ist baulich von den restlichen Räumen getrennt;
- Der Zutritt zum Rechenzentrum ist nur autorisierten Personen gestaltet; das Rechenzentrum ist durch einen dreifachen Verschluss gesichert;
- Der Zutritt ist durch Kontrolle des Personalausweises sichergestellt. Die Daten werden beim Einlass als sog. Whitelist geführt. So wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können; Mitarbeiter erhalten Zugang über ihren Transponder, soweit es zur Aufgabenerfüllung erforderlich ist.

- Das Zutrittskontrollsystem, sowie die vorhandenen Alarmanlagen sind durch eine USV gegen Stromausfall gesichert;
- In allen sensiblen Bereichen befinden sich Bewegungsmelder;
- Das Rechenzentrum wird regelmäßig innerhalb eines vorgegebenen Zeitfensters durch Personal begangen.

cc. Der Auftraggeber nutzt darüber hinaus weitere **Rechenzentrumsflächen am Standort Karlsruhe** (Rechenzentrum IPC3), für welches folgende Maßnahmen getroffen wurden:

- Die Außentüren sind mit Transponder-Schließsystem mit individualisierten Berechtigungen ausgestattet und grundsätzlich verschlossen; das Gebäude verfügt über ein Zwei-Faktor-Zugangssystem (Transponder und PIN);
- Der Zutritt ist durch Kontrolle des Personalausweises sichergestellt. Die Daten werden beim Einlass als sog. Whitelist geführt. So wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können;
- Das Gebäude ist mit einer Alarmanlage gesichert, welche von einer Sicherheitszentrale 24/7 überwacht wird; der Zutritt zum Rechenzentrum ist nur autorisierten Personen gestaltet;
- Alle Gebäudeschächte sind durch bauliche Maßnahmen abgesichert;
- Alle Zugänge zum Haus sind videoüberwacht und werden aufgezeichnet.
- In allen sensiblen Bereichen befinden sich Bewegungsmelder;
-

b. Der Auftragnehmer verhindert durch die nachfolgenden Maßnahmen, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)

Alle Datenverarbeitungssysteme sind vor unberechtigten Zugang geschützt. Dies erfolgt insbesondere dadurch, dass

- Mitarbeiter ausschließlich mit personalisierten Benutzerprofilen arbeiten;
- ein Rechte- und Rollenkonzept beim Auftragnehmer etabliert ist;
- die Authentifikation der Mitarbeiter an den Arbeitsstationen über biometrische Verfahren vorgenommen wird, als auch mit Benutzername / Passwort über Windows AD
- alle Arbeitsplatz-PCs durch Sicherheitsschlösser physisch gesichert sind;
- der Zugang zur Kunden-Verwaltungsoberflächen mindestens einem Passwort geschützt sind;
- alle eingesetzten Systeme sich hinter einer mehrfach redundanten Hardware-Firewall befinden;
- alle Systeme mit besonderem Gefährdungspotential zusätzlich jeweils über eine eigene Software-Firewall verfügen;
- alle mobilen Datenträger und Laptops, auf denen personenbezogene Daten verarbeitet werden, verschlüsselt sind;
- alle Mitarbeiter durch eine Richtlinie angehalten werden, komplexe Passwörter zu verwenden und diese nach definierten Zeiträumen zu ändern; die Einhaltung der Kriterien automatisiert überprüft wird;

c. Der Auftragnehmer trägt Sorge dafür, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass die personenbezogenen Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Die unerlaubten Zugriffe in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen wird im Besonderen verhindert dadurch, dass

- alle zu internen Zwecken eingesetzten Systeme des Auftragnehmers durch regelmäßige Sicherheitsupdates auf dem aktuellen Stand gehalten werden;
- Zugriffsrechte nur für erforderliche Verarbeitungsvorgänge und personenbezogene Daten vergeben werden; hierfür besteht ein Berechtigungskonzept;
- Administratorzugänge auf das Notwendigste beschränkt sind;
- der Zugriff auf Anwendungen protokolliert wird und die Möglichkeit besteht, diese Daten auszuwerten;
- Datenträger die temporär nicht genutzt werden, sicher in einem dafür vorgesehenen Tresor aufbewahrt werden;
- Datenträger, die für einen anderen Zweck eingesetzt werden sollen, nach einem definierten Verfahren mehrfach überschrieben (gelöscht) werden;
- Datenträger, welche nicht weiter verwendet werden, nach einem definierten Verfahren nach DIN 66399 gelöscht werden;
- die Aktenvernichtung über einen zertifiziertes Unternehmen erfolgt; die Vernichtung wird protokolliert.

d. Der Auftragnehmer trägt Sorge dafür, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Trennungskontrolle)

Die getrennte Datenverarbeitung wird gewährleistet durch:

- Trennung der Daten wird erreicht durch physische oder logische unterschiedliche Speicherung;
- Klare Trennung von Kundenzugriffen (logische Trennung durch individuelle Benutzerprofile mit Passwortschutz)
- Test- und Produktivsystem getrennt sind.

2. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO)

Für die Pseudonymisierung ist der Auftraggeber verantwortlich.

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

a. Dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass es überprüft und festgestellt werden

kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist (Weitergabekontrolle)

Die unberechtigte Weitergabe personenbezogener Daten wird insbesondere hierdurch umgesetzt:

- Die Datenkommunikation wird verschlüsselt (z.B. VPN, SSL) oder es werden eigene Standleitungen verwendet;
- Die Datenkommunikation zwischen unterschiedlichen Auftraggebern wird vom Auftraggeber logisch getrennt; ist dies nicht möglich, wird die Kommunikation durch eine VPN-Verbindung verschlüsselt;
- Der Transport von E-Mails erfolgt grundsätzlich verschlüsselt;
- Alle Mitarbeiter sind i.S.d. Art. 32 Abs. 4 DSGVO unterwiesen und verpflichtet;
- Beim physischen Transport werden die Transportpersonen sorgfältig ausgewählt; es werden verschlossene und speziell gesicherte Transportbehälter verwendet
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

b. Dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

Diese Kontrolle erfolgt durch:

- Protokollierung von Eingaben, Änderungen und Löschungen von Daten (insbesondere durch Logfiles)
- Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Die Zugriffsrechte orientieren sich an der Erforderlichkeit für die Aufgabenerfüllung
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) ist gegeben.
- Formulare, aus denen Daten in automatisierte Verarbeitungen übernommen wurden, werden aufbewahrt.
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (Verfahrensanweisung).

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

a. Dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

Die Verfügbarkeit bei internen Systemen des Auftragnehmers wird insbesondere durch folgende Maßnahmen umgesetzt:

- Es besteht für alle Server, auf denen personenbezogene Daten gespeichert werden, eine unterbrechungsfreie Stromversorgung (USV); am Standort Karlsruhe ebenfalls Dieselgeneratoren mit einer Überbrückungszeit von 96 Stunden.

- Die Klimatisierung wird redundant vorgehalten.
- Alle Server, sowie die Temperatur und Feuchtigkeit in den Serverräumen werden automatisiert überwacht (Erreichbarkeitsprüfung von außen, sowie Zugriffs-Versuche bei Servern).
- Schutzsteckdosenleisten in Serverräumen.
- Die Rechenzentrumsflächen verfügen über Feuer- und Rauchmeldeanlagen; der Alarm wird automatisiert an eine Sicherheitszentrale gemeldet, welche 24/7 besetzt ist.
- Automatische Brandlöschanlage mit Schutzgas sowie ausreichende Anzahl an Feuerlöschern in elektrischen Betriebsräumen und im Rechenzentrum.
- Es besteht ein Backup-Konzept mit täglicher Datensicherung aller relevanten Daten; die Datenwiederherstellung wird regelmäßig getestet; Aufbewahrung der Datensicherungen auf LTO Bändern an einem sicheren, ausgelagerten Ort außerhalb der Bürogebäude des Auftragnehmers
- Für alle Serversysteme bestehen entsprechende Dokumentationen, die eine Wiederherstellbarkeit ermöglichen.
- Es besteht eine Richtlinie, wie Notfälle zu erkennen sind und wohin diese gemeldet werden müssen.
- Regelmäßige Wartung und Funktionskontrolle (vierteljährlich) durch Fachfirma nach DIN VDE 0833

b. Dafür Sorge zu tragen, dass die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt ist.

Die Belastbarkeit wird durch folgende Maßnahmen sichergestellt:

- Alle relevanten Systeme werden von außen auf mögliche Angriffsszenarien getestet
- Relevante Systeme werden redundant vorgehalten

5. Fähigkeit, die Verfügbarkeit rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DS-GVO)

Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Die Fähigkeit wird durch folgende Maßnahmen sichergestellt:

Für alle internen Systeme ist definiert, wer im Falle einer Nichtverfügbarkeit der Systeme zu informieren ist, um die Systeme schnellstmöglich wiederherzustellen.

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

a. Der Auftragnehmer hält ein Datenschutz-Management-System vor, welches laufend verbessert wird.

Dies umfasst unter anderem:

- Eine Datenschutzleitlinie der Unternehmensleitung
- Richtlinien zum Umgang mit personenbezogenen Daten und der zugehörigen IT für alle Mitarbeiter
- Verfahren die den konkreten Umgang mit personenbezogenen Daten regeln.
- Bestellung eines externen Datenschutzbeauftragten
- Regelmäßige Kontrolle durch den Datenschutzbeauftragten
- Regelmäßige Schulung und Aufklärung, um das Problembewusstsein zu fördern
- Gelegentliche unangekündigte Kontrollen, ob die Datenschutz- und Datensicherungsmaßnahmen eingehalten werden.

b. Der Auftragnehmer hat ein Incident Response Management umgesetzt

Dies umfasst unter anderem:

- Richtlinien für Mitarbeiter, wie mit möglichen Sicherheitsvorfällen umzugehen ist
- Verfahren, wie die verantwortliche Stelle mit festgestellten oder gemeldeten Sicherheitsvorfällen umzugehen hat, insbesondere, wann der Datenschutzbeauftragte und die Datenschutzbehörde zu involvieren ist.

c. Der Auftragnehmer trägt Sorge dafür, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen (Auftragskontrolle)

Dies wird erreicht durch:

- Sorgfältige Auswahl von Auftragsverarbeitern in Zusammenarbeit mit dem Datenschutzbeauftragten
- Detaillierte Regelung zum Auftragsverhältnis (insbesondere wirksame Kontroll- und Zugriffs- und Löschungsrechte)
- Regelmäßige Kontrollen durch den Datenschutzbeauftragten

Der Auftraggeber gewährleistet, dass eine Leistungserbringung in deutschen Rechenzentren und unter Beachtung des DSGVO erfolgt.