Vertrag zur Auftragsverarbeitung

Zwischen

Auftraggeber

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

BSA Systemhaus GmbH

Teramostraße 36

87700 Memmingen

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich

Service und Wartung von Drucksystemen

auf Grundlage des Hauptvertrags. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die den Datenschutz betreffenden Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 2. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Für Leistungen, die nicht vom Hauptvertrag geregelt werden, kann der Auftragnehmer für diese Tätigkeiten eine Vergütung gegenüber dem Auftraggeber geltend machen.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 4 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen die in Anlage 4 aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 5 dargestellt.

§ 5 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 7 aufgeführten Maßnahmen der

1. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
4. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter/als Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DS-GVO nicht bestellt werden muss) bestellt:

Rechtsanwältin und TÜV zertifierte Datenschutzbeauftragte Sabine Schenk

von der Anwaltskanzlei Schenk Datenschutz Rechtsanwaltsgesellschaft mbH

Phone: 08333 / 926936-0

Fax: 08333 / 926936-1

Anschrift:

Auf der Wies 18

87727 Babenhausen

Zweigstelle:

Zweigstr. 10 (Nähe Karlsplatz / Stachus)

80336 München

Phone: 089 / 21543877

Email: info@europajurist-schenk.com

Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Beim Auftraggeber ist als betrieblicher Datenschutzbeauftragter/als Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DS-GVO nicht bestellt werden muss) bestellt: vgl. **Anlage 6**

(5) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Auftraggebers durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder

Textform informieren. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

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

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind. Soweit diese Auskünfte die Leistungen des Hauptvertrages überschreiten, ist der Auftragnehmer berechtigt, für diese Leistungen einen Vergütungsanspruch gegenüber dem Auftraggeber geltend zu machen.

(4) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(5) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält.

(6) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das im Rahmen der DS-GVO festgelegte Recht, sich von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum

Auftragnehmer steht. Der Auftraggeber hat die Kosten der Kontrollen selbst zu tragen. Darüber hinaus ist der Auftragnehmer berechtigt für Unterstützungsleistungen bei den Kontrollen einen Vergütungsanspruch gegenüber dem Auftraggeber geltend zu machen. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 3 genannten Subunternehmer durchgeführt. Der Auftraggeber stimmt den in Anlage 3 genannten Subunternehmern zu. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Es wird geregelt, dass die Auslagerung auf Subunternehmer zulässig ist, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und

Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils - gegebenenfalls anteilig - von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht oder nur anteilig für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 11 Änderung und Ergänzung dieser Vertragsbedingungen

(1) Der Auftragnehmer ist berechtigt, diese Vertragsbedingungen zu ändern oder zu ergänzen soweit dies aufgrund von

1. Änderungen und Neuerungen der maßgeblichen Gesetze, insbesondere der DSGVO und des BDSG (n.F.) oder der entsprechenden Rechtsprechung oder

2. technischen Weiterentwicklungen, aus denen sich eine Veränderung der Datenverarbeitung oder Datensicherheit ergibt,

geschieht.

(2) Der Auftragnehmer wird dem Auftraggeber die Änderungen oder Ergänzungen spätestens sechs Wochen vor ihrem Wirksamwerden schriftlich ankündigen. Ist der Auftraggeber mit den

Änderungen oder Ergänzungen der Vertragsbedingungen nicht einverstanden, so kann er der Änderungen oder Ergänzungen innerhalb einer Frist von zwei Wochen in Textform widersprechen (Eingangsfrist). Erfolgt kein solcher Widerspruch, so gelten die Änderungen oder Ergänzungen der Vertragsbedingungen als vom Auftraggeber genehmigt. Der Auftragnehmer wird den Auftraggeber mit der Mitteilung der Änderungen oder Ergänzungen der Vertragsbedingungen auf die vorgesehene Bedeutung seines Verhaltens und das Widerspruchsrecht besonders hinweisen.

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer.

(2) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Die Anlagen 1 -7 werden Bestandteil dieses Vertrags.

(5) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist München.

Anlagen

Anlage 1 – Beschreibung der Dienstleistung

Anlage 2 – Weisungsberechtigte Personen bei den jeweiligen Vertragsparteien

Anlage 3 – Genehmigte Subunternehmer

Anlage 4 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 5 – Beschreibung der Betroffenen/Betroffenengruppen

Anlage 6 – Datenschutzbeauftragter des Auftraggebers

Anlage 7 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 1 – Beschreibung der Dienstleistung

Der Auftragnehmer ist gegenüber dem Auftraggeber nach Maßgabe des Hauptvertrages zur Bereitstellung, Instandhaltung und Wartung von Drucker- und Multifunktionssystemen verpflichtet. Der Zweck der Drucker- und Multifunktionssysteme ist die Verarbeitung von Dokumenten in elektronischer oder in Papierform.

Der Auftragnehmer hat nur in Ausnahmefällen Zugriff auf personenbezogene Daten des Auftraggebers oder von Dritten. Dies vor allem in Fällen der Bereitstellung der Drucker- und Multifunktionssysteme, bei der Instandhaltung und Wartung der Drucker- und Multifunktionssysteme (z.B. zwischenzeitliche Datenübertragung auf ein anderes Gerät, um das bestehende Gerät zu reparieren oder zu ersetzen) und bei einer eventuellen Geräteübernahme nach Vertragsende. Eine weitere Verarbeitung von personenbezogenen Daten des Auftraggebers durch den Auftragnehmer außer den genannten Fällen erfolgt grundsätzlich nicht.

Nach Vertragsende wird eine gesonderte Vereinbarung zwischen Auftraggeber und Auftragnehmer getroffen, ob das Gerät zerstört, gelöscht oder die Festplatte entnommen/ausgebaut und an den Auftraggeber übergeben werden soll. In diesen Fällen kann es zu einem Zugriff auf personenbezogenen Daten des Auftraggebers durch den Auftragnehmer kommen, jedoch werden die personenbezogenen Daten des Auftraggebers durch den Auftragnehmer nur nach Weisung des Auftraggebers und zum Zweck der gewünschten Datenverarbeitung des Auftraggebers durch den Auftragnehmer verarbeitet.

Die Zulässigkeit der Datenverarbeitung beurteilt zu jedem Zeitpunkt der Auftraggeber.

Anlage 2 – Weisungsberechtigte Personen bei den jeweiligen Vertragsparteien

Weisungsberechtigte Personen bei Auftraggeber	Weisungsberechtigte Personen bei Auftragnehmer
	Gerhard Breher
	Christoph Fischer
	Marcus Hasse

Anlage 3 – Genehmigte Subunternehmer

Dienstleitungsunternehmen/ Subunternehmer	Anschrift/ Sitz	Art der Auftragsverarbeitung
pcvisit Software AG	Manfred-von-Ardenne-Ring 20, D-01099 Dresden	Fernwartungssoftware
Walko Transporte GmbH	Schussentalstr. 53 88255 Baienfurt	Transporte
Rettinger-Transporte	Am Steg 17, 86971 Peiting	Transporte

Anlage 4 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien:

Die Art und Zweck der von der Zugriffsmöglichkeit des Auftragnehmers betroffenen Daten hängt von dem Inhalt des Gerätespeichers ab.

Art der Daten
Personenstammdaten (z.B. Namen)
Kommunikationsdaten (z.B. Telefon, E-Mailadresse)
Vertragsstammdaten (z.B. Vertragsbeziehung)
Kundenhistorie
Bankdaten (z.B. IBAN)
Kreditkartendaten (z.B. Kreditkartennummer)
Vertragsabrechnungs- und Zahlungsdaten
IP-Adresse
Auskunftsangaben (z.B. von Dritten aus öffentlichen Verzeichnissen)
Planungs- und Steuerungsdaten
Besondere Arten von personenbezogenen Daten

Anlage 5 – Beschreibung der Betroffenen/Betroffenengruppen

Kategorien betroffener Personen
Kunden
Interessenten
Abonnenten
Beschäftigte (Art. 88 DS-GVO; § 26 BDSG n.F.)
Lieferanten
Handelsvertreter
Ansprechpartner
Minderjährige als Beschäftigte, Auszubildende, Praktikanten

Anlage 6 – Datenschutzbeauftragter des Auftraggebers (vom Auftraggeber auszufüllen)

Name, ggf. Unternehmen, Anschrift, E-Mail, Telefon, Fax:

_____

_____

_____

_____

_____

Anlage 7 – Technische und organisatorische Maßnahmen des Auftragnehmers:

Inhaltsverzeichnis

1. Zutrittskontrolle

Maßnahmen um den Zutritt zu Datenverarbeitungsanlagen durch Unbefugte zu verhindern (z.B. physische Barrieren wie verschlossene Türen).

Maßnahmen (an allen Standorten: Teramostr. 36, 87700 Memmingen; Sudetenstraße 9, 87600, Kaufbeuren; Katharinengasse 34, 86150, Augsburg; Kreuzäcker 4, 88214, Ravensburg):

- Es besteht ein Berechtigungskonzept. Dieses legt die Sicherheitszonen fest und stellt sicher, dass berechtigten Personen nur zu den ihrer Berechtigung entsprechenden Sicherheitszonen Zutritt gewährt wird.
- Zutrittsrechte zu den gesicherten Objekten und Bereichen haben ausschließlich Angestellte des Auftragnehmers.
- Die Eingangstüren und Nebentüren zum Gebäude sind durch mit Bolzen verriegelte Sicherheitstüren gesichert, so dass ein Schutz vor unbemerktem Betreten/Verlassen der Gebäude besteht. Ein Schließkonzept ist vorhanden.
- Die Serverräume sind nochmals gesondert gegen den Zutritt unberechtigter Personen, insbesondere auch außerhalb der Geschäftszeiten, geschützt. Sie verfügen über keine Außenfenster und werden weder durch Schächte noch durch Aufzüge tangiert. Der Zutritt zu den Serverräumen wird durch eine Schlüsselregelung für Unbefugte verwehrt. Schlüssel besitzt nur ein überschaubarer Kreis von Mitarbeitern des Auftragnehmers. Externe Dienstleister erhalten nur nach Aufforderung und im Beisein befugter Personen Zutritt.
- Der Eingangsbereich wird durchgehend von mehreren Empfangsmitarbeitern überwacht.
- Besucher werden in den Gebäuden beaufsichtigt. Besucher werden nach Identitätsfeststellung zum Besuchten begleitet bzw. von ihm abgeholt.

2. Zugangskontrolle

Maßnahmen, um den Zugriff auf Datenverarbeitungssystemen durch Unbefugte zu verhindern (z.B. Passwörter, Schutz gegen Hacker).

Maßnahmen:

Um die DV-Anlage vor Eindringlingen zu schützen, werden Verfahren der Identifikation und Authentifikation eingesetzt, welche den Zugang steuern:

- Die Anmeldung erzwingt vor Zugriff auf Daten oder Programme die Eingabe Passwortes (Authentifizierung) verbunden mit einer Benutzerkennung (Identifizierung), sodass eine 2-Faktor-Authentisierung vorliegt. Eine gegenüber dem System durchgeführte fehlerhafte Autorisierung führt nach einer definierten Anzahl von Versuchen zur Sperrung des Zugangs zum System. Zudem sind einzelne Programme nochmals mittels eigenem Passwortes und Benutzerkennung gesichert.
- Bei Erstanmeldung ist eine Passwortänderung erforderlich.
- Zur Durchsetzung sicherer Passwörter sind eine Mindestlänge von 6 Zeichen, die Verwendung von Zeichen, Zahlen und Sonderzeichen, sowie ein automatischer Verfall alle 40 Tage technisch vorgegeben. Ehemalige Passwörter werden 8 Generationen in einer Passwort-Historie gespeichert, um die erneute Verwendung durch denselben Berechtigten zu vermeiden.
- Die Passwörter und Benutzerkennungen werden verschlüsselt abgespeichert.

Zudem werden Verfahren zur Aufdeckung von Unregelmäßigkeit zwecks Erkennung unberechtigter Nutzung angewandt:

- Anmeldeversuche werden protokolliert.

Die Zugangsberechtigungen werden wie folgt verwaltet:

- Für die Vergabe von Benutzerkennungen und Kennwörtern bestehen schriftliche Regelungen und Verfahrensweisen.

Außerdem findet automatisch eine Bildschirmsperrung nach 10 Minuten Inaktivität statt.

3. Zugriffskontrolle

Maßnahmen, um zu gewährleisten, dass der Zugriff auf Daten nur durch den jeweils zum Zugriff auf diese konkreten Daten Berechtigten erfolgt (z.B. Berechtigungsverwaltung).

Maßnahmen:

- Die Zugriffsrechte werden nach dem „Need-To-Know“ Prinzip vergeben. Es werden nur so viele Zugriffsrechte vergeben, wie für die Wahrnehmung der Aufgaben der jeweiligen Rolle notwendig sind.
- Die Berechtigung wird automatisch anhand der Benutzerkennung geprüft.
- Für sensible Daten besteht ein gesondertes Laufwerk mit beschränktem Zugriff darauf. Außerdem Bestehen differenzierte Rollen mit unterschiedlichen Bearbeitungsrechten (Lesen, Schreiben, Ändern oder Löschen bezogen auf Dateien, Satzgruppen und Datenfelder).
- Die Nutzer können nur auf freigegebene Software zurückgreifen.
- Die Zugriffsberechtigungen werden von einem kleinen, für das jeweilige System verantwortlichen Mitarbeiterkreis vergeben.
- Die Verwendung privater Datenträger zu geschäftlichen Zwecken und die Mitnahme geschäftlicher Datenträger zu privaten Zwecken sowie die Verwendung geschäftlicher Datenträger im privaten Bereich sind verboten.

4. Weitergabekontrolle / Übermittlungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

- Beim Transport von Datenträgern vom Sitz der Auftragnehmerin an andere Orte werden die Datenträger verschlüsselt. Das entsprechende Passwort wird dem Empfänger auf einem anderen Weg übermittelt. Der Transport erfolgt entweder persönlich, per Kurier oder mit vergleichbaren Transportdiensten.
- Daten werden mittels Datenübertragungsleitungen nur konzernintern in einem VPN-Tunnel übermittelt. Die Authentifizierung der VPN-Endpunkte geschieht durch Nutzung öffentlicher Schlüssel.

- Der Empfang, die Benutzung, die Entfernung und die Ausgabe von mobilen Datenträgern ist beschränkt auf schriftlich definierte Mitarbeiter. Die Ausgabe von mobilen Datenträgern erfolgt nur an autorisierte Personen und gegen schriftlichen Nachweis. Der Nachweis wird mindestens 90 Tage aufbewahrt.
- Als allgemeine Sicherheitsmaßnahmen werden VPN, Firewall, Antivirenprogramm, sowie Zusatzsoftware zur Gewährleistung des Zugriffschutzes, zur Gewährleistung der elektronischen Signatur und zur Virenbekämpfung eingesetzt.
- Es ist den Mitarbeitern die Mitnahme, Installation und Inbetriebnahme von privater Software und Hardware an den Arbeitsplatz untersagt.
- Den Mitarbeitern ist es untersagt, virenverdächtige Anhänge zu öffnen.
- Datenträger werden, sobald sie nicht mehr benötigt werden, in einem dokumentierten Verfahren durch einen zertifizierten Entsorger vernichtet. Über die Vernichtung werden schriftliche Protokolle geführt. Soweit personenbezogene Daten auf Papier oder optischen oder magnetischen Datenträgern verarbeitet werden, werden die Objekte sobald sie nicht mehr benötigt werden, in den vorhandenen verschlossenen Datenschutzbehältern entsorgt oder in einen Schredder gegeben, der unter Aufsicht einer befugten Person steht.
- Mitarbeiter sind auf Geheimhaltung und Vertraulichkeit verpflichtet worden. Darüber hinaus erfolgen geschäftsspezifisch weitere Verpflichtungen. Weisungsgebundenheit, Hinweispflichten und Prüfungsrechte sind vertraglich geregelt. Eine Schulung sowie eine schriftliche Bestätigung durch die Mitarbeiter darüber ist erfolgt.
- Bei Versetzung oder Ausscheiden eines Mitarbeiters werden die nicht mehr benötigten (im Falle des Ausscheidens alle) Zugangsberechtigungen entzogen.
- Die Fernwartung erfolgt über einen VPN-Tunnel und ist zusätzlich durch Secure ID, Benutzerkennung und Passwort gesichert. Fernwartungsmöglichkeiten werden nur im Einzelfall freigegeben und vom Auftraggeber initiiert. Nur benannte Mitarbeiter sind hierzu berechtigt. Es besteht eine vertragliche Grundlage für die Fernwartung.
- Die Fernwartung und damit der Zugriff auf ein ortsfremdes Gerät wird lediglich unter der Voraussetzung der Einwilligung des Besitzers durchgeführt. Der Kreis des autorisierten Wartungspersonals ist auf die IT-Abteilung festgelegt. Dem Personal des Auftragnehmers werden nur solche Zugriffsmöglichkeiten eröffnet, die für die Fehlerbehebung unbedingt erforderlich sind. Im Rahmen der Wartung bzw. der Fernwartung werden keine Funktionen freigeschaltet, die eine Übertragung oder Auswertung von Anwenderdatenbeständen zulassen. Die Wartung wird lediglich von sachkundigen Mitarbeitern vorgenommen.

5. Verfügbarkeit und Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem Zwischenfall rasch wiederhergestellt werden können.

Maßnahmen:

- Von allen Daten wird täglich eine Totalsicherung angefertigt. Die Sicherungskopien werden räumlich getrennt von den Datenverarbeitungsanlagen in einem separaten Brandabschnitt sowie außerhalb der Räume der Auftragnehmerin aufbewahrt. Die erforderlichen Systempasswörter sind hinterlegt.
- Es sind in den Serverräumen Brandmelder installiert und in den Serverräumen und überall in den Gebäuden Feuerlöscher verfügbar.
- Die Serverräume sind gegen Einbruch durch eine verschließbare Tür geschützt.

6. Auftragskontrolle / Vertragskonformitätskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO verpflichtet. Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind zudem hinsichtlich des Datenschutzes belehrt und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.
- Sollte die BSA Systemhaus GmbH bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO i. V. m. Art 32 Abs. 1 DSGVO.

7. Datentrennung

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden. Dies gewährleistet auch die Zweckbindung der Datenverarbeitung.

Maßnahmen:

Daten von verschiedenen Auftraggebern werden strikt getrennt. Die Verarbeitung der personenbezogenen Daten in separaten Bereichen mit unterschiedlichen Zugriffs- und Umgangsrechten sorgt so für die „informationelle Gewaltenteilung“. Zudem besteht ein gesondertes Laufwerk für sensible Daten.

8. Prüfung der Betriebsorganisation und Rechenschaftspflicht

Maßnahmen:

- Es ist ein Datenschutzbeauftragter schriftlich bestellt, der ist die innerbetriebliche Organisation regelmäßig überprüft, sodass deren Gestaltung den besonderen Anforderungen des Datenschutzes gerecht wird.
- Ein prozessualisierter Umgang mit Sicherheitsvorfällen ist implementiert. Im Falle eines Vorfalls informieren die Mitarbeiter die IT bzw. ihren Vorgesetzten unverzüglich. Im Anschluss erfolgt die Abstimmung mit dem Datenschutzbeauftragten. Die Bearbeitung durch diesen ist durch entsprechende Vertretungsregelungen sichergestellt.
- Die BSA Systemhaus GmbH nutzt ein erstelltes Datenschutzmanagement-System (DSMS), in dem alle Maßnahmen, Verfahren sowie Tätigkeiten im Bereich des Datenschutzes abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).
- Die BSA Systemhaus GmbH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus, sowie der schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter.
- Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO verpflichtet. Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind zudem hinsichtlich des Datenschutzes belehrt und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.