Allgemeinen Bedingungen zur Auftragsdatenverarbeitung der Computer Sommer GmbH – V2 14.02.2023

1. Allgemeines

Gegenstand der Vereinbarung ist die Vereinbarung der Rechte und Pflichten des Kunden (nachfolgend auch „Auftraggeber") und der Computer Sommer GmbH (nachfolgend auch „Auftragnehmer" oder „Computer Sommer" genannt) sofern im Rahmen der Leistungserbringung eine Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten für den Kunden durch Computer Sommer erfolgt.

2. Gegenstand und Dauer des Auftrages

Computer Sommer verarbeitet im Rahmen des IT-Service personenbezogene Daten im Auftrag des Kunden. Der Umfang der Tätigkeit ergibt sich aus dem Hauptvertrag sowie aus etwaigen Einzelweisungen. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

3. Konkretisierung des Auftragsinhalts

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

Computer Sommer erhebt, verarbeitet und nutzt personenbezogene Daten, welche Mitarbeiter im Rahmen von Dienstleistungen und Reparaturen erheben und verarbeiten. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 – 50 EU-DSGVO erfüllt sind.

3.2 Art der Daten/Kreis der Betroffenen

Die Art und Menge der genutzten personenbezogenen Daten und betroffenen Personengruppen hängt vom Einsatz/Nutzung des Leistungsgegenstandes des Hauptvertrages ab. Folgende Arten von Daten können betroffen sein: Softwarebenutzerdaten, Mitarbeiterdaten, Kundendaten. Der Kreis der Betroffen sind: Mitarbeiter und Kunden des Auftraggebers.

4. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle,

Computer Sommer GmbH
Erwitter Straße 151 · 59557 Lippstadt
Telefon (0 29 41) 28 70-0 · Fax (0 29 41) 28 70-70
Geschäftsführer: Jürgen Schumacher, Oliver Strupath
Amtsgericht Paderborn HRB 5478
Umsatzsteuer-ID DE125688151

Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots, sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung etc., die im **ANHANG 1** „Datenschutzkonzept der Computer Sommer GmbH" gesondert beschrieben werden. Diese technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach Artikel 30 Abs. 2 EU-DSGVO dem Auftraggeber zur Verfügung zu stellen.

5. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach Artikel 28 EU-DSGVO folgende Pflichten:

- Schriftliche Bestellung, soweit gesetzlich vorgeschrieben, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Abschnitt 4 EU-DSGVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

- Die Wahrung des Datengeheimnisses entsprechend Artikel 28 Abs. 3 b EU-DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend. Artikel 32 EU-DSGVO.

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Artikel 57 und 58 EU-DSGVO. Dies gilt auch, soweit eine zuständige Behörde nach. Artikel 57 und 58 EU-DSGVO beim Auftragnehmer ermittelt.

- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) vorlegen.

7. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Ziffer 6 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt. Die im **ANHANG 2** enthaltenen Subunternehmer sind für den Auftragnehmer mit den vorgenannten Auftragsinhalten in dem dort genannten Umfang tätig. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Computer Sommer ist berechtigt, mit einer angemessenen Ankündigungsfrist diese Subunternehmer gegen andere Subunternehmer auszutauschen. Dabei werden die Interessen des Kunden angemessen berücksichtigt. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung Artikel 28 Abs. 3 d i. V. m. Artikel 28 Abs. 2 und 4 EU-DSGVO beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Ebenso sind Hersteller von Softwaremodulen (z. B. Plug-ins oder Add-ons) bzw. Integrationen, die lediglich eine von Computer Sommer zur Verfügung gestellte Schnittstelle nutzen, keine Subunternehmer im Sinne dieser Vereinbarung.

8. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Artikel 32 EU-DSGVO vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig (mindestens 7 Werktage vorher) anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Der Auftraggeber lässt die Kontrolle nur durch eine Person durchführen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragnehmers, dessen Ausstattung, Geschäftsgeheimnisse und Sicherheitsmaßnahmen verpflichtet ist. Der Auftragnehmer behält sich vor, etwaig entstehende interne oder externe Kosten für diese Kontrollen in den Geschäftsräumen des Auftragnehmers dem Auftraggeber in Rechnung zu stellen. Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Artikel 28 Abs. 3 h) EU-DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen Art. 32 EU-DSGVO nach und stellt alle erforderlichen Informationen dazu zur Verfügung. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) erbracht werden.

9. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Es ist bekannt, dass nach Art. 33 und 34 EU-DSGVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 32 bis 36 EU-DSGVO treffen, hat der Auftragnehmer ihn hierbei mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen.

10. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (Art. 28 Abs. 3 a) EU-DSGVO). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich, per E-Mail (in Textform) oder per Fax bestätigen. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer hat den Auftraggeber unverzüglich (Art. 28 Abs. 3, letzter Absatz) zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Der Auftragnehmer ist berechtigt (aber nicht verpflichtet), die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber schriftlich oder per Telefax bestätigt oder geändert wird.

11. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, vorbehaltlich anderer vertraglicher Absprachen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Wahrung von Geschäftsgeheimnissen

Die Parteien verpflichten sich zu strikter Vertraulichkeit Dritten gegenüber. Die Parteien sind insbesondere verpflichtet, alle ihnen anlässlich der Durchführung des Auftrags bekanntwerdenden Geschäfts- und Betriebsgeheimnisse, Herstellungsverfahren, Arbeitsmethoden und sonstigen geschäftlichen bzw. betrieblichen Tatsachen, Unterlagen und Informationen der anderen Partei sowie ihrer Kunden und Geschäftspartner streng vertraulich zu behandeln, in keiner Weise Dritten zugänglich zu machen oder sonst zu verwenden, vorbehaltlich anderer vertraglicher Absprachen. Die Weitergabe solcher Informationen ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig. Die vorgenannte Verpflichtung findet insoweit keine Anwendung, als die Partei darlegen kann, dass Informationen öffentlich zugänglich und zum Zeitpunkt der Offenlegung verfügbar oder danach der Öffentlichkeit zugänglich geworden sind, und zwar ohne

Verletzungshandlung oder -unterlassung durch diese Partei oder eines ihrer Vertreter oder Angestellten, oder vor dem Erhalt von der anderen Partei im Besitz der Partei oder ihr bekannt waren, oder der Partei durch eine andere Person ohne Einschränkung rechtmäßig offen gelegt wurden, oder von der Partei ohne Zugang zur Information der anderen Partei unabhängig entwickelt wurden, oder nach gesetzlichen oder verwaltungsrechtlichen Vorschriften offen gelegt werden müssen, wenn der anderen Partei dieses Erfordernis unverzüglich bekannt gegeben wird und der Umfang solcher Offenlegung soweit wie möglich eingeschränkt wird, oder aufgrund einer gerichtlichen Entscheidung offen gelegt werden müssen, wenn der anderen Partei von dieser Entscheidung unverzüglich Nachricht gegeben wurde und wenn nicht die Möglichkeit besteht, diese Entscheidung anzufechten.

13. Kontaktpersonen

Soweit Weisungen oder Hinweise nach dieser Vereinbarung gegenüber der jeweils anderen Partei gegeben werden, sind sie an Oliver Strupath bei Computer Sommer als Weisungsberechtigten oder -empfänger zu richten und an die im Auftrag als Weisungsberechtigten oder -empfänger für den Kunden genannte Person zu richten. Jede Partei kann einseitig ihre Kontaktpersonen durch schriftliche Erklärung gegenüber der anderen Partei ändern.

Computer Sommer GmbH
Erwitter Straße 151 · 59557 Lippstadt
Telefon (0 29 41) 28 70-0 · Fax (0 29 41) 28 70-70

Geschäftsführer: Jürgen Schumacher, Oliver Strupath
Amtsgericht Paderborn HRB 5478
Umsatzsteuer-ID DE125688151

ANHANG 1 zu den Allgemeinen Bedingungen zur Auftragsdatenverarbeitung

Datenschutzkonzept:
Technische und organisatorische Maßnahmen (früher Anlage zu § 9 BDSG)
der Computer Sommer GmbH

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Der Zutritt in das Unternehmen erfolgt über ein zentrales Schließsystem. Dieses wird bei Verlust eines Schlüssels ausgetauscht. Innerhalb des Gebäudes sind einzelne Räume durch spezielle Schlösser vor unbefugten Zutritt geschützt. Für die Vergabe der verschiedenen Schlüsselarten ist ein autorisierter Mitarbeiter zuständig. Die Vergabe der einzelnen Schlüssel orientiert sich an den verschiedenen Positionen der Mitarbeiter und wird in einer Schlüsselliste dokumentiert.

Das Gebäude verfügt über vier Eingänge bzw. Ausgänge: den Haupteingang, den Personaleingang, das Lager und den Fluchtweg (Feuertreppe). Lediglich der Haupteingang ist während der Geschäftszeiten geöffnet. Durch die sich im Eingangsbereich befindende Verkaufstheke wird sichergestellt, dass sich firmenfremde Personen nur in Begleitung von Mitarbeitern in den Geschäftsräumen bewegen können. Außerhalb der Geschäftszeiten ist das Unternehmen durch eine Alarmanlage gesichert. Die Alarmanlage hat eine direkte Schaltung zu einem Wachdienst-Unternehmen.

Der Serverraum des Unternehmens befindet sich in einem fensterlosen Raum des Gebäudes. Zutritt zu dem Serverraum hat nur die Geschäftsleitung und die Systemadministratoren. Dieser Raum ist durch eine Sicherheitstür gegen unbefugten Zutritt gesichert. Die Reinigung des Serverraums erfolgt während der Geschäftszeiten durch einen der Systemadministratoren. Für die Wartung und die Reinigung der Klimaanlage in dem Serverraum ist die spezialisierte Wartungsfirma „Kälte- und Klimatechnik Koch" verantwortlich. Ebenso wie bei dem Serverraum ist der Zutritt zu den Patchräumen und zu dem Archiv des Unternehmens durch einen separaten Bereich der Schließanlage abgegrenzt. Zutritt zu den Patchräumen hat die Geschäftsleitung und die Systemadministratoren. Für das Archiv sind die Buchhaltung und die Geschäftsleitung zutrittsberechtigt.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Der Serverraum, die Patchräume und das Archiv sind im Zugang beschränkt.

Alle Rechner des Unternehmens sind durch Benutzerprofile mit Passwort vor unberechtigtem Zugriff geschützt. Die Passwörter können nur durch Systemadministratoren zurückgesetzt werden. Die Benutzerprofile unterliegen verschiedenen Benutzergruppen und Berechtigungen.

Computer Sommer GmbH
Erwitter Straße 151 · 59557 Lippstadt
Telefon (0 29 41) 28 70-0 · Fax (0 29 41) 28 70-70
Geschäftsführer: Jürgen Schumacher, Oliver Strupath
Amtsgericht Paderborn HRB 5478
Umsatzsteuer-ID DE125688151

Der Zugriff auf das Unternehmensnetzwerk von außen ist durch VPN, eine Hardware-Firewall und Security-Software geschützt. Mobile Datenträger haben eine 256-Bit-AES-Verschlüsselung.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Es liegt ein anwenderbezogenes Berechtigungskonzept vor. Die Berechtigungen können auf Dateien, auf Datensätze, auf Anwendungsprogramme und das Betriebssystem differenziert werden und die Lese-, Änderungs- und Löschrechte einschränken. Es wird sichergestellt, dass jeder Benutzer nur auf die Daten zugreifen kann, zu denen er zugriffsberechtigt ist. Das Berechtigungskonzept, das sich an den Stellungen der Mitarbeiter orientiert, ist schriftlich festgehalten. Verschiedene Zugriffsrechte werden durch vorgefertigte Benutzerprofile zusammengefasst. Weiterhin ist das Berechtigungskonzept programmtechnisch in der Anwendung und im Active Directory hinterlegt. Die Zugriffe der Benutzer werden protokolliert. Alle Rechner des Unternehmens melden sich nach einer bestimmten Zeit der Inaktivität automatisch ab.

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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.

Die personenbezogenen Daten des Unternehmens werden im Bereich der Lohnbuchhaltung an die Krankenkassen, die Banken und das Finanzamt und im Bereich der Finanzbuchhaltung an den Steuerberater und das Finanzamt übermittelt. Zur Weitergabe personenbezogener Daten sind nur die Mitarbeiter der Personalabteilung berechtigt.

Die Übertragung via VPN ist durch IP/Sec gesichert. Weiterhin findet eine Übertragung personenbezogener Daten ausschließlich über gesicherte Verbindungen statt.

5. Eingabe Kontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Zur Gewährleistung der Eingabekontrolle sind die vom Softwarehersteller mitgebrachten Log Mechanismen und Transaktionsprotokolle, zur Protokollierung aller Eingaben für alle Anwendungen, vorhanden.

6. Auftragskontrolle

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

Der Umgang mit Subunternehmern beginnt mit einer sorgfältigen Auswahl. Auswahlkriterien sind die Sicherheit, die Zuverlässigkeit, die Erfahrung und der Umgang mit Datenschutz und Datensicherheit. Bevor wir Subunternehmer beauftragen werden diese von uns eingehend geprüft. Jeder Dienstleister, der mit personenbezogenen Daten in Kontakt kommt, wird vertraglich dazu verpflichtet alle Anforderungen der Datenschutz-Grundverordnung (i. S. d. Art. 28 EU-DSGVO) einzuhalten. Subunternehmer dürfen prinzipiell nur mit schriftlicher Weisung arbeiten, vernichten personenbezogene Daten nach Beendigung des Vertragsverhältnisses, verpflichten ihre Mitarbeiter auf das Datengeheimnis und bestellen einen Datenschutzbeauftragten. Diese Überprüfungen unterliegen einem ständigen Prüfprozess.

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Daten auf dem Server werden zentral gesichert und die Datensicherung wird stetig dokumentiert. Das realisierte Datensicherungskonzept definiert die Anzahl der Sicherungskopien, dem Umfang der zu sichernden Daten, die Zeitintervalle und die Zeitpunkte der Sicherung. Darüber hinaus wird durch das Konzept die Anzahl der aufbewahrten Generationen und die/der Art/Ort zur Aufbewahrung festgelegt. Die Datensicherungsbänder werden in den Büroräumlichkeiten der für die Datensicherung verantwortlichen Person in einem Tresor sowie durch sichere Auslagerung aufbewahrt. Die Geschäftsleitung, die verantwortliche Person und die Systemadministratoren verfügen über entsprechende Zugriffsrechte. Zur Datensicherung der Daten auf den Laptops tragen die Benutzer der entsprechenden Geräte die Verantwortung zum Ablegen der Daten auf dem Server. Das Unternehmen setzt eine unterbrechungsfreie Stromversorgung ein, in der Blitz- und Überspannungsschutz integriert sind.

Andere Speichermedien des Unternehmens (DVD, Streamer, externe Festplatten) werden in abschließbaren Schränken, im Tresor oder durch sichere Auslagerung aufbewahrt.

Es werden regelmäßig aktualisierte Virenscanner und eine regelmäßig kritisch überprüfte Firewall eingesetzt. Alle Server sind durch Unterbrechungsfreie Stromversorgung (USV) gegen Stromausfall gesichert. Im Serverraum ist eine Klimaanlage im Einsatz. Darüber hinaus sind Geräte zur Überwachung von Temperatur und Feuchtigkeit installiert.

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Es wird eine physikalische Trennung von verschiedenen speichernden Stellen realisiert. Weiterhin wird eine Trennung organisatorisch durchgeführt.

ANHANG 2 zu den Allgemeinen Bedingungen zur Auftragsdatenverarbeitung

Zugelassene Subunternehmer:

Im Folgenden die Liste der Subunternehmer, welche Dienstleistungen für die Computer Sommer GmbH erbringen:

Name	Bereich	Sitz
Terra Cloud GmbH	Cloud Dienstleistungen	32609 Hüllhorst
Netcup GmbH	Webhosting	76185 Karlsruhe
Büroorganisation Strothkamp GmbH	Druckerservice	59494 Soest

Computer Sommer GmbH
Erwitter Straße 151 · 59557 Lippstadt
Telefon (0 29 41) 28 70-0 · Fax (0 29 41) 28 70-70

Geschäftsführer: Jürgen Schumacher, Oliver Strupath
Amtsgericht Paderborn HRB 5478
Umsatzsteuer-ID DE125688151