Zusatzvereinbarung zur Auftragsdatenverarbeitung

zum Vertrag / zu den Verträgen unter der

Kundennummer: _____

zwischen

Firma: _____

Name: _____

Straße: _____

PLZ / Ort: _____

nachfolgend

- **Auftraggeber / Kunde** -

und

Werbeagentur Carra
Inh. Markus Carra-Neubauer
Buckenhofener Str. 54a
91301 Forchheim

nachfolgend

- **Auftragnehmer** -

Werbeagentur Carra
Inh. Markus Carra-Neubauer
Buckenhofener Str. 54a
91301 Forchheim

Telefon: 0 91 91 / 97 82 84
Telefax: 0 91 91 / 97 82 83

Mail: service@carra.de
Web: www.carra.de

Bankverbindung:
Sparkasse Forchheim
Konto: 810 1 826
BLZ: 763 510 40

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Hauptvertrag (Angebot / Leistungsbeschreibung, AGB) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

§ 1 Definitionen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst folgende Tätigkeiten: Hostingleistungen für Webhosting-Pakete, Online-Festplatten, Internet-Shops, dedizierte und virtuelle Server. Die Leistungen umfassen je nach Paket die Bereitstellung von Speicherplatz, elektronischen Postfächern, Datenbanken und Skripten sowie Backups. Des Weiteren erstellt der Auftragnehmer Websites, Online Shops, WebApps, Mobile Apps und sonstige Anwedungen im Bereich Webdesign und Programmierung. Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser Dienstleistungen. Dies umfasst Tätigkeiten, die in den Angeboten / Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO)). Die Art der personenbezogenen Daten und der Verarbeitungszweck werden in **Anlage 1** näher beschrieben.

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe seiner Daten verlangen, soweit der Auftraggeber dies mit seinen Zugriffen nicht selbst durchführen kann.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf die Daten des Auftraggebers (Anlage 1) nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten / Aufwendungen vom Auftraggeber zu tragen.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Auflistung dieser technischen und organisatorischen Maßnahmen wird als **Anlage 2** beigefügt.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten. Den Aufwand für die Erteilung der Auskünfte hat der Auftraggeber zu tragen.

(4) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen:

Ansprechpartner:

Markus Carra-Neubauer, Buckenhofener Str. 54a, 91301 Forchheim

Telefon: 09191 – 978282
E-Mail: datenschutz@carra.de

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten, soweit die Daten des Auftraggebers betroffen sind.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Die Kosten für den entstehenden Aufwand beim Auftragnehmer trägt der Auftraggeber.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. daten- schutzrechtlicher Bestimmungen feststellt.

(3) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend. Die Kosten für den entstehenden Aufwand beim Auftragnehmer trägt der Auftraggeber.

(4) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses liegt beim Auftraggeber.

(5) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen:

Name: _____

Anschrift: _____

Telefon: _____

E-Mail: _____

(6) Die Daten werden nach dem Ende des jeweiligen Vertrages gelöscht. Es obliegt dem Auftraggeber, Sicherungskopien von seinen Daten anzufertigen und die Daten vor Vertragsende umzuziehen. Der Auftraggeber hat selbst Zugriff auf seine Daten. Eine Pflicht des Auftragnehmers zur Herausgabe besteht daher nicht.

§ 5 Anfragen Betroffener an den Auftraggeber

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortetwird.

§ 6 Kontrollrechte

(1) Der Auftraggeber kann sich auf seine Kosten vor der Aufnahme der Datenverarbeitung und sodann jederzeit von den technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. In der Regel erfolgt diese Überzeugung durch die Einholung von Selbstauskünften des Auftragnehmers oder die Vorlage eines Zertifikates des Auftragnehmers.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind. Die entstehenden Kosten hierfür können dem Auftragnehmer in Rechnung gestellt werden.

(3) Sollte dem Auftraggeber die Selbstauskunft - etwa wegen der Sensitivität der verarbeiteten Daten oder des Gefährdungspotentials -, nicht ausreichen, kann der Auftraggeber sich durch einen anerkannten Sachverständigen für IT-Datenschutz (TÜVPrüfer oder vergleichbar) vor Ort von den technischen und organisatorischen Maßnahmen überzeugen. Die Kontrolle vor Ort kann nur nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs erfolgen. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(4) Der Auftraggeber kann die Ergebnisse der Prüfung dokumentieren und die Ergebnisse / Dokumentation für den Nachweis der Erfüllung seiner Sorgfaltspflichten verwenden, soweit Geheimhaltungsinteressen oder Sicherheitsinteressen des Auftragnehmers dem nicht entgegenstehen. Der Auftraggeber ist sich bewusst, dass jede weitere Verwendung Geheimhaltungsinteressen und Sicherheitsinteressen des Auftragnehmers gefährden und diesem Schaden zufügen kann. Die Geheimhaltungspflicht besteht auch im Interesse aller anderen Kunden, weil die Veröffentlichung der Sicherheitsmaßnahmen die Sicherheit der Rechenzentren gefährdet. Keinesfalls dürfen Ergebnisse Dritten mitgeteilt oder veröffentlicht werden.

(5) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 3 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungspflichten verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. dritte Unternehmen mit Leistungen unterbeauftragt.

(2) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Der Auftragnehmer prüft die Unterauftragnehmer mindestens einmal jährlich, um sicherzustellen, dass die nötigen Datenschutz-Maßnahmen getroffen wurden.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 3 genannten Subunternehmer durchgeführt. Der Auftraggeber stimmt zu, dass der Auftragnehmer weitere Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber.

§ 8 Informationspflichten, Annahmeerklärung, Schriftformklausel, AGB

(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 Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Änderungen und Ergänzungen dieser Zusatzvereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Es gilt deutsches Recht.

(5) Im Übrigen gelten die Allgemeinen Geschäftsbedingungen des Auftragnehmers.

(6) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Werbeagentur Carra

Anlagen

Anlage 1 - Auflistung der personbezogenen Daten und Zweck ihrer Verarbeitung

Anlage 2 - Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen

Anlage 3 - Angaben zu Unterauftragsverarbeitern

Anlage 1 - Auflistung der personbezogenen Daten und Zweck ihrer Verarbeitung

1. Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder –nutzung

Datenverarbeitungszweck ist die Erbringung der technischen Leistungen für die Bereitstellung der Dienstleistungen der Werbeagentur Carra, wie sie in den Angeboten / Leistungsbeschreibungen und den AGB der Werbeagentur Carra beschrieben werden.

2. Art der Daten*

Daten, die der Auftraggeber oder von ihm autorisierte Nutzer in den bereit gestellten Paketen (Webhosting-Pakete, Online-Speicher, E-Shops, dedizierte und virtuelle Server) speichern (Inhalt der Webseiten, des Online-Speichers, der Datenbanken, E-Mails etc.)

☐ Adressdaten	☐ Abrechnungsdaten	☐ E-Mails
☐ Angebotsdaten	☐ Finanzdaten	☐ Video- / Bilddateien
☐ Bankverbindungsdaten	☐ Mitarbeiterdaten	☐ Nutzungsdaten
☐ Bestelldaten	☐ Leistungsdaten	☐ Interessen / Profile
☐ Kontaktdaten	☐ Personalverwaltung	☐ Authentifizierungsdaten
☐ Vertragsdaten	☐ Gesundheitsdaten	☐ Transaktionsdaten
☐ Stammdaten	☐ _____	☐ _____
☐ _____	☐ _____	☐ _____

3. Kreis der von der Datenerhebung, -verarbeitung oder –nutzung Betroffenen*

☐ Kunden	☐ Mitarbeiter	☐ Angehörige
☐ Nutzer	☐ Auszubildende	☐ Unterhaltsberechtigte
☐ Interessenten	☐ Bewerber	☐ Ruheständler
☐ Kontaktpersonen	☐ Praktikanten	☐ Pressevertreter
☐ Lieferanten / Dienstleister	☐ frühere Mitarbeiter	☐ Geschädigte
☐ Geschäftspartner	☐ Berater	☐ Zeugen
☐ Gesellschafter	☐ Mitglieder	☐ Mieter
☐ Makler / Vermittler	☐ _____	☐ _____
☐ _____	☐ _____	☐ _____

* vom Auftraggeber auszufüllen

Anlage 2 - Darstellung der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO und Anlage

In diesem Dokument beschreiben wir die wesentlichen technischen und organisatorischen Sicherheitsmaßnahmen, die wir zum Schutz Ihrer Daten ergreifen. Aus Sicherheitsgründen geben wir nur eine allgemeine Beschreibung, denn der beste Schutz Ihrer Daten ist die Geheimhaltung der genauen Sicherheitsmaßnahmen. Soweit erforderlich, sinnvoll und wirtschaftlich werden die wesentlichen Systeme mit den beschriebenen Maßnahmen ganz oder teilweise ausgestattet. Die Sicherheit und Verfügbarkeit unseres Rechenzentrums wird regelmäßig nach DIN ISO 27001 geprüft. Datenschutz und Datensicherheit sind für uns von zentraler Bedeutung. Die Sicherheitsmaßnahmen werden kontinuierlich an den technischen Fortschritt und die aktuellen Gefährdungsszenarien angepasst.

1. Zutrittskontrolle Rechenzentrum

Zutritt	Anforderung	Status
Allgemeine Regelung Zutrittskontrolle	Regelung des Zutritts zu Datenverarbeitungs-anlagen	Die Maßnahmen zur Zutrittssicherheit sind abhängig vom Einsatzzweck der Räumlichkeiten und dem Schutzbedarf der Systeme, die sich in ihnen befinden. Sensible Datenverarbeitungsanlagen befinden sich immer in entsprechend geschützten Räumlichkeiten wie z. B. den Rechenzentren („**RZ**“) des Anbieters. Grundlegende Maßnahmen folgen im Weiteren und sind detailliert im Dokument Anforderungen Zutrittssicherheit definiert.
Schutz der Räume mit Datenverarbeitungsan-lagen vor dem Zutritt Unbefugter	Eingezäuntes Betriebsgelände	Die Betriebsgelände der Rechenzentren sind umzäunt.
	Alarmanlage, Videoüberwachung	Sensible Gebäude bzw. Gebäudeteile werden mit einer Videoanlage, z. T. mit Bewegungsmeldern und einer Einbruchmeldeanlage überwacht.
	Personenkontrolle beim Gebäudezutritt	Es existieren technische und organisatorische Maß-nahmen zur Beschränkung des Zutritts zu geschützten Bereichen für interne und externe Personen. Dies umfasst die Kontrolle der Zutritte per Besucherliste, Tragepflicht von Mitarbeiter- und Gästeausweisen und stete Begleitung von Gästen. Ebenso existiert ein Rechtesystem für den Zutritt zu besonders schützenswerte Bereichen.
	Zutrittskontrollsystem	Die Zutrittssteuerung im RZ-Standort erfolgt über ein Zutrittskontrollsystem (Transponderkarten mit elektronischem Türöffner, bei RZ-Zutritt zusätzlich PIN). Das System regelt und kontrolliert den Zutritt zum Grundstück und zu den Gebäuden.
	Schlüsselregelung / Schlüsselbuch	Die Schlüsselausgabe erfolgt durch den Wachdienst oder das zentrale Gebäudemanagement. Jeder ausgegebene Schlüssel wird in einem Schlüsselbuch oder einem Schlüsselmanagementsystem vermerkt.
	Weitere Überwachungsein-richtungen	Im RZ: 7 x 24 Stunden Wachdienst inkl. regelmäßigen Kontrollgängen; Videoüberwachung und Bewegungsmelder in den RZ-Fluren

2. Zutrittskontrolle Werbeagentur

Der Zugang ist durch eine Außentür (Hauseingang) und durch die Eingangstür gesichert. Die Schlüsselvergabe erfolgt durch den Geschäftsführer und ist im Schlüsselverzeichnis geregelt.

3. Zugangskontrolle Rechenzentrum

Zugang	Anforderung	Status
Schutz der Computersysteme gegen den Zugang für Unbefugte	Zugang zu Systemen nur über Zugangsberechtigungen	Zum Zugang zu Systemen muss sich der Nutzer grundsätzlich mittels eines Verfahrens auf dem aktuellen Stand der Technik authentisieren. Bei Systemen mit besonders hohem Schutzbedarf bzw. kritischen Zugriffswegen sind zusätzliche Verfahren, wie z. B. eine Zwei-Faktor-Authentifizierung, etabliert. Fernwartungszugriffe und hier notwendige zusätzliche Maßnahmen sind in der „Fernwartungsrichtlinie“ dokumentiert.
	Berechtigungen nur nach Genehmigung	Die Zugangsberechtigung wird beantragt und von dem verantwortlichen Vorgesetzten und / oder dem Informationseigner genehmigt. Besondere Berechtigungen (z. B. Systemadministrator) bedürfen zudem der Genehmigung durch Beauftragte. Je nach Vereinbarung ist zusätzlich eine Genehmigung durch den Kunden erforderlich.
	Bedarfsbezogene Berechtigung	Der Zugang zu Applikationen und zu Informationen erfolgt auf Basis von Rollen und dem konkreten geschäftlichen Bedarf der Benutzer (Prinzip der minimalen Berechtigung/Need To Know Prinzip).
	Kennwortverfahren	Das Kennwortverfahren ist in der Kennwortrichtlinie dokumentiert. Passwortlänge, Komplexität, Gültigkeit und Historie werden verbindlich vorgegeben und die Vorgaben werden kontinuierlich an aktuelle Anforderungen angepasst.
	Protokollierung und Kontrolle fehlerhafter Anmeldungen	Fehlerhafte Anmeldungen werden soweit sinnvoll und technisch machbar protokolliert und bei Bedarf oder nach Kundenvereinbarung ausgewertet.
	Automatische Sperrung PC (z. B. Kennwort oder Pausenschaltung)	Eine automatische Sperrung des PC erfolgt nach einem festgelegten Zeitraum.
	Zugang zu Netzwerken	Unsichere Netze („**untrusted**“, z. B. Internet) wer-den durch Security Gateways (Firewalls, Proxy, SMTP-Gateways etc.) separiert und überwacht.
	Zugang über mobile Geräte	Der Zugang über mobile Geräte bzw. deren Einsatz wird über die ISi-Richtlinie und über die „Regeln für mobile Devices“ reglementiert und gesteuert.

4. Zugangskontrolle Werbeagentur

Der Zugang zu Systemen erfolgt mit Authentifizierung durch Benutzerkennung und Passwort. Berechtigungen werden nach einem Zugangsberechtigungskonzept vergeben, die Passwörter müssen den Sicherheitsanforderungen genügen. Die Systeme sind gegen unberechtigten Zugang z.B. durch eine Firewall gesichert.

5. Zugriffskontrolle Rechenzentrum

Zugriff	Anforderung	Status
Schutz der Daten gegen den Zugriff durch Unbefugte	Zugriff auf Daten nur über Zugriffsberechtigungen	Zum Zweck der Zugriffskontrolle erfolgt die Autorisierung von Benutzern über ein Rechte- bzw. Berechtigungssystem.
	Berechtigungsvergabe und -Entzug	Die Zugriffsberechtigung muss beantragt und von dem verantwortlichen Vorgesetzten genehmigt wer-den. Besondere Zugriffsberechtigungen bedürfen zudem der Genehmigung durch Beauftragte. Vergabe und Entzug von Zugriffsberechtigungen werden durch einen elektronischen Workflow unterstützt und dokumentiert. Der Berechtigungsprozess beinhaltet den Entzug von Zugriffsberechtigungen im Falle eines Wechsels in der Verantwortung oder bei Ausscheiden eines Mitarbeiters aus dem Unternehmen.
	Kontrolle der Berechtigungs-vergaben	Eine Kontrolle der Berechtigungsvergaben erfolgt anlassbezogen und regelmäßig im Rahmen interner und externer Audits.
	Kontrollierte Vernichtung von Daten und Ausdrucken	Die kontrollierte Vernichtung von Daten und Ausdrucken erfolgt durch spezialisierte, zertifizierte Dienstleister.

6. Zugriffskontrolle Werbeagentur

Berechtigungen sind in den IT-Systemen festgelegt, differenzierte Zugriffe und differenzierte Berechtigungen werden festgelegt. Der Zugriff entsprechend Berechtigung wird auch bei Verfahren zur Wiederherstellung von Daten aus Backups gewahrt. Test- und Produktionsumgebung sind getrennt. Fernwartungen werden mit Verschlüsselung vorgenommen.

7. Weitergabekontrolle

Alle unsere Mitarbeiter werden auf das Datengeheimnis verpflichtet. Soweit erforderlich werden die Daten gegen Zugriffe auf Netzwerkebene geschützt, Daten verschlüsselt und Schnittstellen gegen unbefugten Datenexport gesichert.

5. Eingabekontrolle

Die Daten werden vom Auftraggeber selbst eingegeben. Unsere Mitarbeiter dürfen grundsätzlich nicht auf Ihre Daten zugreifen bzw. Daten eingeben, verändern oder löschen. Wir nehmen Sperrungen aus rechtlichen oder technischen Gründen sowie im Falle des Zahlungsverzuges vor. Die Vornahme von Sperrungen wird protokolliert. Die Protokolldaten werden aufbewahrt und enthalten die Mitarbeiterkennung. Die Löschung erfolgt nach dem Vertragsende.

6. Auftragskontrolle

Wir schließen auf Wunsch einen schriftlichen Vertrag, der den Datenverarbeitungszweck regelt und ein Weisungsrecht enthält. Unsere Mitarbeiter kennen den Datenverarbeitungszweck. Sie erhalten schriftliche Weisung zum Umgang mit personenbezogenen Daten. Ein IT-Organisationshandbuch / IT-Sicherheitskonzept ist vorhanden. Unterauftragsverhältnisse werden schriftlich beauftragt.

7. Verfügbarkeitskontrolle

Die Rechenzentren verfügen über eine unterbrechungsfreie Stromversorgung durch Batterien und Dieselaggregate. Die Primärtechnik und die wesentliche Sekundärtechnik ist redundant aufgebaut. Backups werden regelmäßig erstellt und die Daten auf getrennten Systemen gespiegelt, soweit dies Leistungsbestandteil ist. Brandmeldeanlagen, Löschanlagen mit Löschgas und ein Notfallplan für die verschiedenen Gefährdungsszenarien sorgen für den physikalischen Schutz Ihrer Daten.

8. Trennungskontrolle

Je nach Paket werden Ihre Daten physikalisch oder logisch / virtuell von anderen Daten getrennt. Die Datensicherung erfolgt auf physikalisch oder virtuell getrennten Einheiten.

9. Pseudonymisierung

Soweit möglich führen eine Pseudonymisierung zum Schutz der Vertraulichkeit durch. Kundendaten, Zugangsdaten und Produktdaten werden getrennt gespeichert.

Anlage 3 – Angaben zu Unterauftragsverarbeitern

Die folgenden Unterauftragsverarbeiter dürfen im Rahmen dieser Vereinbarung eingesetzt werden:

Unternehmer	**Anschrift**	**Tätigkeit**
Dell GmbH	Unterschweinstiege 10, 60549 Frankfurt am Main	Wartung
HP Deutschland GmbH	Herrenberger Str. 140, 71034 Böblingen	Wartung
Netapp GmbH	Sonnenallee 1, 85551 Kirchheim	Wartung
Teamix GmbH	Südwestpark 35, 90449 Nürnberg	Wartung
Technogroup IT-Service GmbH	Feldbergstr. 6, 65239 Hochheim	Wartung
QSC AG	Am Tower 5, 90475 Nürnberg	Wartung, Remote Hands
ARNDT GmbH & Co. KG	Industriestr. 42, 90765 Fürth	Service Desk, Remote Hands, Wartung
Suse Linux GmbH	Maxfeldstr. 5, 90409 Nürnberg	Wartung
Matrix AG	Nymphenburger Str. 1, 80335 München	Wartung
secura Gebäudemanagement GmbH	Oskar-von-Miller Str. 14, 85055 Ingolstadt	Sicherheitsdienst, Remote Hands
InterNetX GmbH	Johanna-Dachs-Str. 55, 93055 Regensburg	Domainservice, Nameserver
Thomas-Krenn.AG	Speltenbach-Steinäcker 1, 94078 Freyung	Wartung
United Hoster GmbH	Nägelestr. 13, 70597 Stuttgart	Hosted Exchange Service
Usercentrics GmbH	Rosental 4, 80311 München	Cookie-Consent-Tool