Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

b&b comtec Garmasch & Gerner GbR
Am Priwall 14 b, 23701 Eutin

als Auftragsverarbeiter/in - nachfolgend "**Auftragnehmer**" genannt –

und

als Verantwortliche/r - nachfolgend "**Auftraggeber**" genannt –

- Auftraggeber und Auftragnehmer nachfolgend jeder auch "Partei" und gemeinsam "Parteien" -

Inhaltsverzeichnis

PRÄAMBEL 2
§ 1 GEGENSTAND/UMFANG DER BEAUFTRAGUNG 2
§ 2 WEISUNGSBEFUGNISSE DES AUFTRAGGEBERS 2
§ 3 SCHUTZMAßNAHMEN DES AUFTRAGNEHMERS 3
§ 4 INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS 3
§ 5 SONSTIGE VERPFLICHTUNGEN DES AUFTRAGNEHMERS 4
§ 6 SUBUNTERNEHMERVERHÄLTNISSE 4
§ 7 KONTROLLRECHTE 5
§ 8 RECHTE DER BETROFFENEN PERSONEN UND DEREN ANFRAGEN 5
§ 9 LAUFZEIT DIESES VERTRAGES 5
§ 10 LÖSCHUNG UND RÜCKGABE NACH VERTRAGSENDE 5
§ 11 HAFTUNG 6
§ 12 SCHLUSSBESTIMMUNGEN 6

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich des IT-Vertriebs (Vertrieb von Hard- und Software) sowie im Bereich der IT-Services (Fehlerdiagnosen, IT-Beratung, IT-Betreuung, Reparatur von Computer und Peripherie, Virenbeseitigung, Datensicherung und -rettung sowie Einrichtung, Konfiguration und Prüfung von EDV-Anlagen, Netzwerktechnik und Telekommunikationstechnik). Die Leistungserbringung stützt sich dabei auf die AGB des Auftragnehmers nebst einer ggf. regelmäßigen Einzelbeauftragungen durch den Auftraggeber (im Folgenden: "**Hauptvertrag"**). Bei der Durchführung des Hauptvertrags kommt es auch zur Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("**DSGVO**"). Zur Erfüllung der Anforderungen der DSGVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Gegenstand/Umfang der Beauftragung

(1) Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "**Auftraggeberdaten**") erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO verarbeitet.

(2) Die **Anlage 1** zu diesem Vertrag enthält eine Auflistung bzgl. Art, Umfang, Zweck der Datenverarbeitung und Kreis der von der Datenverarbeitung betroffenen Personen. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich in dem dort genannten Umfang.

(3) Die Verarbeitung der Auftraggeberdaten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen 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.

§ 2 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung), dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "**Weisungsrecht**"). 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 (z.B. E-Mail) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

(3) Die Parteien teilen der jeweils anderen Partei die Kontaktdaten der weisungs- und empfangsberechtigten Personen mit. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Bis zum Zugang dieser Mitteilung bei der jeweiligen Partei gelten die benannten Personen weiter als weisungs-, und empfangsberechtigt.

(4) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden

als Antrag auf Leistungsänderung behandelt.

(5) 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.

§ 3 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) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden "**Mitarbeiter**" genannt), in Schriftform zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine 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 Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in **Anlage 2** zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 4 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 Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen enthalten jeweils 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 wird den Auftraggeber im Falle des § 4 Abs. 1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierrüber den Auftraggeber und ersucht um weitere Weisungen. Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach

Absatz 1 betroffen sind.

(3) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 3 Abs. 3 wird der Auftragnehmer den Auftraggeber unverzüglich unterrichten.

§ 5 Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung (Verarbeitungsverzeichnis), das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

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

(3) Der Auftragnehmer ist unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen verpflichtet, den Auftraggeber bei er Einhaltung seiner Pflichten aus Art. 32-36 DSGVO zu unterstützen.

(4) Der Auftragnehmer bestätigt, dass er –soweit eine gesetzliche Verpflichtung hierzu besteht- einen Datenschutzbeauftragten bestellt hat. Im Falle der Pflicht zur Benennung eines Datenschutzbeauftragten veröffentlicht der Auftragnehmer die stets aktuellen Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite.

(5) Sollten die Auftraggeberdaten 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DSGVO liegt.

§ 6 Subunternehmerverhältnisse

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis") befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. 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). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(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, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 7 Kontrollrechte

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. 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 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 Anforderung (schriftlich oder in Textform) 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 Rechte der betroffenen Personen und deren Anfragen

(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 DSGVO.

(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.

§ 9 Laufzeit dieses Vertrages

(1) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags bzw. der zwischen den Parteien bestehenden Geschäftsbeziehung. Dieser Vertag gilt aber mindestens solange fort, wie die Geschäftsbeziehung z.B. durch die aufeinanderfolgende Einzelbeauftragung, zwischen den Parteien fortbesteht.

(2) Die vorliegende Vereinbarung bleibt zudem 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.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags bzw. der bestehenden Geschäftsbeziehung oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen und Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags bzw. der bestehenden Geschäftsbeziehung hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

§ 11 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DS-GVO.
(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 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) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren
(4) Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
(5) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Eutin.

_____

Ort, Datum und Unterschriften
b&b comtec Konstantin Garmasch und Ekaterina Gerner GbR

_____

Ort, Datum und Unterschriften (Auftraggeber)

Anlagen:

- Anlage 1: Beschreibung der Art der personenbezogenen Daten, besonderen Kategorien personenbezogener Daten und Kategorien betroffener Personen
- Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers
- Anlage 3: Genehmigte Subunternehmer

Anlage 1

Beschreibung der Art der personenbezogenen Daten, besonderen Kategorien personenbezogener Daten und Kategorien betroffener Personen.

Art der personenbezogenen Daten	**Umfang und Zweck der Datenverarbeitung**	**Kategorien betroffener Personen**
Personenstammdaten: Name, Adresse, E-Mail, Telefonnummer etc.	Fernwartung Datensicherung Datenwiederherstellung Datenvernichtung Systemwiederherstellung Datenbankpflege IT-Support	Privatpersonen Kunden Mitarbeiter Interessenten Lieferanten Ansprechpartner Mandanten von Steuerberatern und Rechtsanwälten
Kundendaten		
Patientendaten (Arzt- / Tierarztpraxen)		
Mandantendaten (Steuerberater/Rechtsanwälte)		

Besondere Kategorien personenbezogener Daten	**Umfang und Zweck der Datenverarbeitung**	**Kategorien betroffener Personen**
Gesundheitsdaten (inkl. genetischer Daten)	Fernwartung Datensicherung Datenwiederherstellung Datenvernichtung Systemwiederherstellung Datenbankpflege IT-Support	Patienten von Arztpraxen
Politische Überzeugung/Meinung	Fernwartung Datensicherung Datenwiederherstellung Datenvernichtung Systemwiederherstellung Datenbankpflege IT-Support	Privatpersonen
Rassische oder ethnische Herkunft		
Religiöse Überzeugung		
Weltanschauliche (philosophische) Überzeugung		
Biometrische Daten zur (eindeutigen) Identifizierung einer Person		
Gewerkschaftszugehörigkeit		
Sexualleben oder sexuelle Orientierung		

Anlage 2

Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle
Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Videoüberwachung
- Schlüsselregelung
- Begleitung von Besucherzutritten durch eigene Mitarbeiter
- Abgestufte Sicherheitsbereiche und kontrollierter Zutritt
- Aufbewahrung der Server in verschlossenen Räumen
- Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen
- Aufbewahrung von Datensicherungen im zutrittsgeschützten Serverschrank
- Anweisung zur Ausgabe von Schlüsseln
- Besetzter Empfang während der Bürozeiten

Zugangskontrolle
Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.

- Verschlüsselung von Netzwerken, Verschlüsselungsalgorithmen:
- Verschluss von Datenverarbeitungsanlagen (verschlossener Cage für Server)
- Passwortsicherung von Bildschirmarbeitsplätzen
- Funktionelle Vergabe von Benutzerberechtigungen
- Verwendung von individuellen Passwörtern
- Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern
- Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
- Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität
- Verpflichtung zur Vertraulichkeit der Mitarbeiter
- Kontrollierte Vernichtung von Datenträgern

Zugriffskontrolle
Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- Festlegung der Zugriffsberechtigung, Berechtigungskonzept
- Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen
- Anforderung)
- Regelmäßige Überprüfung von Berechtigungen
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
- Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)
- Systemseitige Protokollierung von Dateizugriffen
- Systemseitige Protokollierung von Dateilöschungen
- Sicherheitssysteme: Virenscanner, Firewalls, SPAM-Filter
- Verschlüsselte Speicherung der Daten, Verschlüsselungsalgorithmen: AES, RSA: 256 bit

Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Trennung von Kunden mithilfe des Datenbanksystems
- Dateiseparierung bei Datenbanken
- Logische Datentrennung (Auftrag-, Kunden-, Lieferantennummer)
- Verarbeitung der Daten des Auftraggebers und anderer Kunden von unterschiedlichen
- Mitarbeitern des Auftragnehmers
- Datensicherung und -wiederherstellung der Auftraggeber-Daten auf separaten
- Datenträgern (ohne Daten anderer Kunden)

Pseudonymisierung
(Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

- Maßnahmen: Vergabe von Auftragsnummern anstelle der Kundennamen

2. **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

Weitergabekontrolle
Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.

- Welche Versendungsart der Daten besteht zwischen Auftraggeber und Auftragnehmer?
  - Auf Wunsch, E-Mail-Versand mit verschlüsselten ZIP-Dateien oder passwortgeschützter PDF-Datei
  - Datenaustausch über https-Verbindung, verschlüsselter E-Mail-Versand
- Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle
- Festlegung der Bereiche, in dem sich Datenträger befinden müssen
- Verschlüsselung von eigenen Laptopfestplatten
- Kontrollierte Vernichtung von Daten:
  Datenträgerentsorgung - Sichere Löschung von Datenträgern:
  - Vernichtung durch spezielle Software
  - Physikalische Zerstörung Papierentsorgung

  Sicheres Vernichten von Papierdokumenten:
  - Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister

Eingabekontrolle
Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Kennzeichnung erhaltener Datenträger
- Festlegung von Benutzerberechtigungen (Profile)
- Differenzierte Benutzerberechtigungen:
  Lesen, Ändern, Löschen

- Teilzugriff auf Daten bzw. Funktionen
- Feldzugriff bei Datenbanken
- Organisatorische Festlegung von Eingabezuständigkeiten
- Systemseitige Protokollierung von Eingaben/Löschungen
- Verpflichtung auf das Datengeheimnis

3. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

Verfügbarkeitskontrolle
Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Datensicherungs- und Backupkonzepte
- Durchführung der Datensicherungs- und Backupkonzepte
- Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal
- Rauchmelder in Serverräumlichkeiten
- Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten
- Serverschrank mit Abluftsystem
- Blitz-/ Überspannungsschutz
- Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt
- Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft
- Lagerung von Archiv-Speichermedien unter dem Schutzbedarf angemessenen Lagerbedingungen
- CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten
- Aufbewahrung der Daten in Datensicherungsschränken
- USV-Anlage (Unterbrechungsfreie Stromversorgung)
- Widerstandsfähigkeit- und Ausfallsicherheitskontrolle
- Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen. Festplattenspiegelung
- Datenspeicherung auf RAID-Systemen (RAID 1 und höher)
- Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
- Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen.
- Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.
- Cyber-Versicherung

4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**

Kontrollverfahren
Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

- Interne Verarbeitungsverzeichnisse werden mind. jährlich aktualisiert
- Prozesse zur Meldung neuer/veränderter Verfahren
- Es werden datenschutzfreundliche Voreinstellungen gewählt
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen
- Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt

Auftragskontrolle

Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.

- Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
- Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)
- Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (während Vertragsdauer)

Anlage 3

Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind vom Auftraggeber genehmigte Subunternehmer:

Name und Anschrift des Unter-Auftragsverarbeiters	**Beschreibung der Teilleistungen**	**Ort der Leistungserbringung**
TeamViewer Germany GmbH Jahnstr. 30 73037 Göppingen Deutschland	Bereitstellung der Fernwartungssoftware und Infrastruktur	Standort: Deutschland
3CX GmbH Walter-Gieseking-Straße 22 30519 Hannover Deutschland	VoIP Telefonanlage	Standort: Deutschland
TERRA CLOUD GmbH Hankamp 2 32609 Hüllhorst Deutschland	Cloud	Standort: Deutschland
ALL-INKL.COM Neue Medien Münnich Hauptstraße 68 02742 Friedersdorf Deutschland	Hosting	Standort: Deutschland