BLUE:SOLUTION
Wir sind OneQrew

Vertrag zur Auftragsverarbeitung
nach Artikel 28 EU- DSGVO

zwischen

blue:solution software GmbH
Rudolf Melching
Albert-Einstein-Str. 12a DE - 48431 Rheine

im Folgenden: **Auftragnehmer**

und

Firma
Vorname Nachname
Straße und Nummer - PLZ Ort

im Folgenden: **Auftraggeber**

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag zur Leistungserbringung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag zur Leistungserbringung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

1. Gegenstand und Dauer der Verarbeitung

(a) Der Auftragnehmer erbringt folgende Leistungen für den Auftraggeber:
Diese ergeben sich aus dem Hauptvertrag zwischen den Parteien über die primäre (Dienst-)Leistung.

(b) Die Laufzeit dieses Vertrages ist an die Laufzeit des Hauptvertrages zwischen Auftraggeber und Auftragnehmer über die primäre (Dienst-) Leistungen des Auftragnehmers gekoppelt, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

2. Ort der Leistungserbringung

(a) Der Auftragnehmer erbringt die Leistungen nach diesem Vertrag ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

(b) Eine Verlagerung der Tätigkeit oder von Teilen der Tätigkeit in ein Drittland i.S.v. Art 44 DSGVO ist darf nur nach vorheriger schriftlicher Zustimmung des Auftraggebers erfolgen und muss zudem die Vorgaben des Artikel 44 DSGVO erfüllen. Die Zustimmung muss in Schriftform (§ 126 BGB) erteilt werden.

3. Art und Zweck der Verarbeitung

(a) Die Verarbeitung der Daten erfolgt auf folgende Art im Sinne von Artikel 4 Nr. 2 DSGVO und zu folgendem Zweck:

Ergibt sich aus dem Vertrag, insbesondere:

- Bereitstellung von IT-Infrastruktur, sowie Speicherung und Sicherung der Daten im Rahmen der Cloud-Hosting-Dienste des Auftragnehmers.
- Diagnose und Wartung per Fernzugriff, bei denen eine Zugriffsmöglichkeit auf personenbezogenen Daten nicht ausgeschlossen werden kann.

4. Art der Daten und Kategorien der betroffenen Personen

(a) Folgende Arten personenbezogener Daten im Sinne von Artikel 4 Nr.1, 13, 14 und 15 DSGVO werden verarbeitet:

- Personenstammdaten (z.B Name und Anschrift, Bild)
- Kommunikationsdaten (z.B Telefon, E-Mail)
- Vertragsstammdaten (z.b Abrechnungs- und Zahlungsdaten, Bankverbindung)
- Kundenhistorie
- Nutzungsdaten
- Kenndaten (z.B Steueridentifikationsnummer, Ausweisnummer)

(b) Folgende Personenkategorien sind betroffen:

- Kunden
- Interessenten des Auftraggebers
- Beschäftigte des Auftraggebers
- Ansprechpartner
- Personen, deren Daten der Auftragnehmer im Auftrag verarbeitet
- Mieter
- Lieferanten

5. Verantwortlicher; Weisungsbefugnis des Auftraggebers

(a) Der Auftraggeber ist Verantwortlicher im Sinne von Artikel 28 und Artikel 4 Nr. 7 DSGVO. Er ist allein verantwortlich die Wahrung der Rechte der betroffenen Personen nach den Artikeln 12 bis 22 DSGVO.

(b) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(c) Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich auf Weisungen, welche er für datenschutzrechtswidrig hält, hinzuweisen. Er hat sodann mit der Ausführung der Weisung abzuwarten bis der Auftraggeber ausdrücklich eine neue Weisung erteilt oder an der bisherigen festhält.

6. Verschwiegenheitspflicht

(a) Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Pflichten des Auftragnehmers

(a) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(b) 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 DSGVO) 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 Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(c) 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 Art. 33 bis 36 DS-GVO genannten Pflichten.

(d) 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.

(e) 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.

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

(g) 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.

(h) 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.

(i) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(j) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

8. Pflichten des Auftraggebers

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

(b) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

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

9. Sicherheit der Verarbeitung

(a) Auftraggeber und Auftragnehmer treffen technische und organisatorische Maßnahmen, welche geeignet sind, das Risiko für die Verletzung von Rechten und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen zu minimieren und ein dem Risiko angemessenen Schutzniveaus zu schaffen. Dabei sind der Stand der Technik, die Implementierungskosten, der Art, des Zwecks und der Umstände der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere des Risikos zu berücksichtigen.

(b) Die Maßnahmen nach Ziffer 9 a) schließen unter anderem folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall zügig wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertungen und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

(c) Die konkreten Maßnahmen des Auftragnehmers ergeben sich aus Anlage 1 zu diesem Vertrag.

(d) Der Auftragnehmer kann die Maßnahmen jederzeit anpassen oder verändern, sofern sichergestellt ist, dass das bisherige Schutzniveau nicht unterschritten wird. Insbesondere kann er die Maßnahmen an technische und organisatorische Weiterentwicklungen anpassen.

10. Nachweismöglichkeiten

(a) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(b) Durchführung eines Selbstaudits.

(c) Unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung.

(d) Zertifikat zu Datenschutz und/oder Informationssicherheit (z. B. ISO 27001).

(e) Genehmigte Verhaltensregeln nach Art. 40 DS-GVO.

(f) Zertifikate nach Art. 42 DS-GVO.

(g) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(h) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 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.

11. Beauftragung von Subunternehmen

(a) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(b) Im Falle der Zustimmung erteilt der Auftraggeber die allgemeine Genehmigung für den Einsatz von Subunternehmen durch den Auftragnehmer, soweit diese in Bezug auf die Auftragsverarbeitung vertraglich unter Berücksichtigung der jeweiligen Dienstleistung in vergleichbarem Maße verpflichtet sind wie der Auftragnehmer gegenüber dem Auftraggeber und die datenschutzrechtlichen Vorgaben nach DSGVO gewährleisten.

(c) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Hauptvertrag zur Leistungserbringung vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. für Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software in Anspruch nimmt.

(d) Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

(e) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(f) Der Auftragnehmer setzt nur in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ansässige Subunternehmen ein. In einem Drittland i.S.v. Art 44 DSGVO ansässige Subunternehmen dürfen nur nach vorheriger Zustimmung des Auftraggebers erfolgen; diese müssen zudem die Vorgaben des Artikel 44 DSGVO erfüllen.

12. Mitteilungspflicht bei Störungen und Verletzung des Schutzes personenbezogener Daten

(a) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Verstöße gegen datenschutzrechtliche Bestimmungen oder die Festlegungen dieses Vertrages mit, welche von ihm oder von ihn beschäftigten Personen hervorgerufen wurden.

(b) Der Auftragnehmer teilt dem Auftraggeber unverzüglich mit, wenn Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten auftreten.

(c) Der Auftragnehmer unterstützt den Auftraggeber soweit möglich bei der Erfüllung dessen Melde- und Benachrichtigungspflichten nach Artikeln 33 und 34 DSGVO.

13. sonstige Pflichten des Auftragnehmers

(a) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit technischen und organisatorischen Maßnahmen dabei, dass dieser seiner Pflicht zur Beantwortung von Anträgen von Betroffenen auf Wahrnehmung ihrer Rechte nach Abschnitt III der DSGVO nachkommen kann.

(b) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zur Verfügung underteilt Auskünfte, welche für den Nachweis, dass er sich an die vertraglichen und gesetzlichen Vorgaben hält, erforderlich sind.

(c) Der Auftragnehmer ermöglicht dem Auftraggeber oder von diesem Beauftragten Prüfern nach Absprache Kontrollen.

(d) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und derihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Artikel 32 bis 36 DSGVO.

14. Datenlöschung bei Vertragsende

(a) Der Auftragnehmer ist verpflichtet, alle personenbezogenen Daten zu löschen, wenn dieser Vertrag endet. Diese Verpflichtung besteht nicht, sofern eine gesetzliche Pflicht zur Speicherung der Daten besteht.

15. Informationspflichten, Schriftformklausel, Rechtswahl

(a) 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.

(b) 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.

(c) 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.

(d) Es gilt deutsches Recht.

16. Haftung und Schadensersatz

(a) Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.

(b) Soweit keine Haftungsregelung vereinbart wurde, haften Auftraggeber und Auftragnehmer gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

17. Sonstiges

(a) Sollte das Eigentum des Auftraggebers oder die zu verarbeitenden personenbezogenen Daten beim Auftragnehmer durch Maßnahmen Dritter wie Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren oder durch Vergleichbares gefährdet werden, hat der Auftragnehmer den Auftraggeber zu informieren.

(b) Anlagen sind Bestandteil dieses Vertrages.

(c) Änderungen oder Ergänzungen dieses Vertrages und seiner Anlagen bedürfen zu ihrer Wirksamkeit der Schriftform (§ 126 BGB). Dies gilt auch für die Änderung dieses Formerfordernisses selbst.

(d) Für Streitigkeiten aus und im Zusammenhang mit diesem Vertrag gilt der Gerichtsstand, welcher in dem Hauptvertrag zwischen den Parteien bestimmt ist.

Anlagen:
Anlage 1: Technische organisatorische Maßnamen
Anlage 2: Subunternehmer

Rheine, den	Ort, den
_____	_____
(blue:solution software GmbH, Rudolf Melching)	(Firma, Vorname Nachname)

Zeitpunkt der Unterzeichnung:

BLUE:SOLUTION
Wir sind OneQrew

Anlage 1:

Technische und organisatorische Maßnahmen zum Vertrag über Auftragsverarbeitung

zwischen

blue:solution software GmbH
Rudolf Melching
Albert-Einstein-Str. 12a DE - 48431 Rheine

im Folgenden: **Auftragnehmer**

und

Firma
Vorname Nachname
Straße und Nummer - PLZ Ort

im Folgenden: **Auftraggeber**

In Erfüllung der Verpflichtungen aus Ziffer 9 des Vertrages zur Auftragsverarbeitung sind folgende technischen und organisatorischen Maßnahmen getroffen:

(1) Organisationskontrolle:

Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Folgende Maßnahmen bestehen:

- Schulung und Sensibilisierung der Mitarbeiter
- Regelung von Verantwortlichkeiten
- Verpflichtungen und Dienstanweisungen
- Verfahrens-, Dokumentations- und Programmierrichtlinien - Funktionstrennung

(2) Zugangskontrolle:

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können, wie beispielsweise Verwehrung des Zugangs Unbefugter zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird.

Folgende Maßnahmen bestehen:

- Absicherung der Gebäude, Fenster und Türen
- Sicherheitsglas
- Bruch- und Öffnungsmelder
- Videoüberwachungs-Anlagen
- Alarmanlagen
- Zutrittskontroll-Systeme mit Chipkarten-Leser
- Passwortrichtlinien
- Zwei-Faktor-Benutzeranmeldung
- Firewalls
- digitale Zertifikate
- Schutz vor Schadsoftware
- Bildschirmsperre
- aktuelle Nutzerverwaltung

(3) Datenträgerkontrolle:

Maßnahmen, die verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Verschlüsselung von Daten und Datensystemen
- Verschlüsselung von Datenträgern
- Kontrollierte Vernichtung von Datenträgern - Absicherung der Daten / Datenträger bei Versand

(4) Speicherkontrolle:

Maßnahmen, die die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten verhindern. Folgende Maßnahmen bestehen:

- Kennwortrichtlinie
- Nutzerprofile und Rollenkonzept entsprechend des Sicherheits- und Berechtigungskonzepts

(5) Benutzerkontrolle:

Maßnahmen die verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können. Folgende Maßnahmen bestehen:

- Kennwortrichtlinie
- Nutzerstammdatensatz
- Sperrung von Systemen - Kontrolle der Verbindungen

(6) Zugriffskontrolle:

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

- Festlegung und Prüfung der Zugriffsberechtigungen
- Protokollierung von Zugriffen
- zeitliche Begrenzung von Zugriffen
- revisionsfähige Dokumentation der Benutzerprofile

(7) Übertragungskontrolle:

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Folgende Maßnahmen bestehen:

- Verschlüsselung und VPN für Zugriff von außen durch Mitarbeiter
- CDs & Sticks mit geeigneten Schutzmechanismen (Verschlüsselung)
- E-Mails mit Transportverschlüsselung
- Ausgangs-Rechnungen mit digitaler Signatur
- VPN-Tunnel

(8) Eingabekontrolle:

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.

Folgende Maßnahmen bestehen:

- Standardmäßig Protokollierung von inhaltlichen Änderungen und bei Änderungen in internen Systemen

(9) Transportkontrolle:

Maßnahmen, die verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Folgende Maßnahmen bestehen:

- Verschlüsselung von Datenträgern (USB, Festplatten, Bänder…)
- Verschlüsselung von Datensystemen (Laptop, Mobiltelefon…) - Verschlüsselung von Übertragungsverbindungen (SSL, TSL…)

(10) Wiederherstellbarkeit:

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Folgende Maßnahmen bestehen:

- Regelmäßige Backup-Verfahren nach dem Backup-Konzept - Daten-Spiegelung in externe Systeme

(11) Zuverlässigkeit:

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Folgende Maßnahmen bestehen:

- Systemanalysen
- Netzüberwachung
- Überwachung der Lebensdauer von Datenträgern

(12) Datenintegrität:

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Folgende Maßnahmen bestehen:

- Prüfsummen
- Zeitstempel
- Signaturen
- Protokolle

(13) Auftragskontrolle:

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

Folgende Maßnahmen bestehen:

- Eindeutige vertragliche Regelung entspr. Art 28 DSGVO
- Verträge mit Auftragsverarbeitern
- Vertragsausführung wird durch den DSB gewährleistet

(14) Verfügbarkeitskontrolle:

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

Folgende Maßnahmen bestehen:

- Regelmäßige Backup-Verfahren nach dem Backup-Konzept
- USV
- RAID Systeme
- Aktuelle Firewall-Lösung auf allen betriebenen Systemen (Server und Clients) - Aktueller Virenschutz auf allen betriebenen Systemen (Server und Clients)

(15) Trennungsgebot:

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

Folgende Maßnahmen bestehen:

- Mandantenfähiges System