Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

Firma: _____

Straße: _____

PLZ Ort: _____

als Verantwortlicher (nachfolgend „Auftraggeber“ genannt)

und

CHC ONLINE / SOLVA
Christian Henkel
Friedrich-Ebert-Str. 147
34119 Kassel

als Auftragsverarbeiter (nachfolgend „Auftragnehmer“ genannt)

§ 1 Vertragsgegenstand und Laufzeit

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des als Anlage 1 angefügten Vertrages („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien den vorliegenden Vertrag. Die Regelungen des vorliegenden Vertrages gehen im Zweifel den Regelungen des Hauptvertrages vor.

(2) Die Laufzeit dieses Vertrages richtet sich nach der Dauer der Verarbeitung.

§ 2 Gegenstand und Dauer der Verarbeitung

(1) Der Gegenstand der Verarbeitung ist in Anlage 1 dargestellt.

(2) Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrages. Die Verarbeitung kann über die Laufzeit des Hauptvertrages hinaus bis zur Rückgabe und Löschung bzw. Vernichtung der personenbezogenen Daten des Auftraggebers andauern.

§ 3 Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung durch den Auftragnehmer sind in Anlage 1 dargestellt.

§ 4 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Die Art der personenbezogenen Daten sind in Anlage 2 dargestellt.

(2) Die Kategorien betroffener Personen sind in Anlage 3 dargestellt.

§ 5 Weisungsrecht

(1) Der Auftragnehmer darf personenbezogene Daten nur auf Weisung des Auftraggebers verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag und den Hauptvertrag festgelegt und können vom Auftraggeber danach in Schriftform oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

(3) Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung. Ist der Auftragnehmer jedoch 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.

§ 6 Verpflichtung zur Vertraulichkeit

Der Auftragnehmer wird alle Personen, die von ihm mit der Verarbeitung von personenbezogenen Daten betraut werden, zur Vertraulichkeit verpflichten (Art. 28 Abs. 3 lit. b DS-GVO).

§ 7 Sicherheitsmaßnahmen

(1) Der Auftragnehmer trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers, insbesondere mindestens die in Anlage 4 aufgeführten Maßnahmen der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Über wesentliche Änderung der Sicherheitsmaßnahmen hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

§ 8 Subunternehmer

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden auch unter Einschaltung von Subunternehmern durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieses Vertrages zu verpflichten. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).

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

§ 9 Unterstützungspflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen nachzukommen.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DS-GVO.

§ 10 Rückgabe und Löschung bzw. Vernichtung

(1) Der Auftragnehmer wird nach Beendigung des Hauptvertrages alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen bzw. vernichten oder zurückgeben und die vorhandenen Kopien löschen bzw. vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

§ 11 Kontrollrechte

(1) Der Auftragnehmer stellt dem Auftraggeber auf Verlangen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten des Auftragnehmers nach diesem Vertrag und nach Art. 28 DS-GVO zur Verfügung.

(2) Der Auftragnehmer ermöglicht dem Auftraggeber hierzu auch Überprüfungen - einschließlich Inspektionen -, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei. Der Auftraggeber wird Überprüfungen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

§ 12 Geheimhaltung

Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu halten und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Informationen Dritten zugänglich zu machen. Dies gilt nicht für Informationen, die der anderen Partei bereits bekannt waren, die sie von Dritten erhalten hat oder welche allgemein öffentlich bekannt sind.

§ 13 Sonstiges

(1) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(2) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Aufraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Für den Auftraggeber:	Für den Auftragnehmer:
	Kassel, 16.05.2018
_____	_____
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift
	Christian Henkel
_____	_____
Vor-, Nachname in Druckbuchstaben	Vor-, Nachname in Druckbuchstaben

CHC ONLINE I SOLVA
Christian Henkel
Friedrich-Ebert-Str. 147
D-34119 Kassel

Telefon +49 561 788085-0
Telefax +49 561 788085-88
E-Mail info@chc-online.de
Internet www.chc-online.de
Marke www.solva.de

Inhaber Dipl.-Oec. Christian Henkel
USt-ID DE 185 162 800

Bankverbindungen
Kasseler Sparkasse (HELADEF1KAS)
IBAN DE11 5205 0353 0002 1205 51
Commerzbank AG (COBADEFF520)
IBAN DE36 5204 0021 0281 1156 00

Anlage 1
Gegenstand, Art und Zweck der Verarbeitung

Je nach der im Hauptvertrag vereinbarten Leistung, werden Gegenstand, Art und Zweck der Verarbeitung wie folgt festgelegt:

§ 1 Domainregistrierung & Hosting & E-Mails

Registrierung und Bereitstellung von Domains und der dazugehörigen Dienste. Bereitstellung von Speicherplatz und Mailservern sowie der dazugehörigen Dienste.

§ 2 Dedizierte Server

Bereitstellung von Servern in einem Rechenzentrum und der zum Betrieb der Server notwendigen Infrastruktur (Strom, Kühlung, Netzanbindung etc.).

§ 3 Managed Services

Einrichtung, Wartung, Konfiguration und Überwachung von Servern, u.a. durch Einspielen von Updates und Austausch von Hardware, zur Gewährleistung der Betriebsbereitschaft der Server.

§ 4 Programmierung von Anwendungen / Internet-Websites

CHC ONLINE I SOLVA
Christian Henkel
Friedrich-Ebert-Str. 147
D-34119 Kassel

Telefon +49 561 788085-0
Telefax +49 561 788085-88
E-Mail info@chc-online.de
Internet www.chc-online.de
Marke www.solva.de

Inhaber Dipl.-Oec. Christian Henkel
USt-ID DE 185 162 800

Bankverbindungen
Kasseler Sparkasse (HELADEF1KAS)
IBAN DE11 5205 0353 0002 1205 51
Commerzbank AG (COBADEFF520)
IBAN DE36 5204 0021 0281 1156 00

Anlage 2
Art der personenbezogenen Daten

Der Auftragnehmer stellt dem Auftraggeber je nach vereinbarten Leistungsumfang Speicherplatz und Server zur Verfügung und erbringt Dienstleistungen in diesem Zusammenhang. Die Art der personenbezogenen Daten, die der Verarbeitung durch den Auftragnehmer unterliegen, ist daher insbesondere davon abhängig, welche Art von personenbezogenen Daten der Auftraggeber auf diesen Servern speichert. Dabei kann es sich insbesondere um nachfolgende allgemeine personenbezogene Daten handeln:

- Adressdaten
- Arbeitszeiten der Beschäftigten
- Bankdaten
- Foto- & Videodaten
- IT-Nutzungsdaten
- Kontaktdaten
- Lohn- und Gehaltsdaten
- Mitarbeiterdaten
- Name
- Persönliche Daten
- Qualifikationsdaten
- Reisedaten
- Standortdaten
- Urlaubsdaten

Auch besondere Kategorien personenbezogener Daten gemäß Artikel 9 DS-GVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DS-GVO können auf diesen Servern gespeichert werden:

- Biometrischen Daten
- Daten über die Gewerkschaftszugehörigkeit
- Daten über politische Meinungen
- Daten über rassische und ethnische Herkunft
- Daten über religiöse oder weltanschauliche Überzeugungen
- Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln
- Daten zum Sexualleben oder zur sexuellen Orientierung
- Genetische Daten
- Gesundheitsdaten

Anlage 3
Kategorien betroffener Personen

Der Auftragnehmer stellt dem Auftraggeber je nach vereinbarten Leistungsumfang Speicherplatz und Server zur Verfügung und erbringt Dienstleistungen in diesem Zusammenhang. Die Kategorien der betroffenen Personen, die der Verarbeitung durch den Auftragnehmer unterliegen, sind daher insbesondere davon abhängig, wessen personenbezogene Daten der Auftraggeber auf diesen Servern speichert. Dabei kann es sich insbesondere um nachfolgende Kategorien betroffener Personen handeln:

- Beschäftigte
- Bewerber
- ehemalige Beschäftigte
- Geschäftspartner
- Interessenten
- Kunden
- Lieferanten/Auftragnehmer
- Newsletter-Abonnenten
- Patienten
- Website-Besucher

CHC ONLINE I SOLVA
Christian Henkel
Friedrich-Ebert-Str. 147
D-34119 Kassel

Telefon +49 561 788085-0
Telefax +49 561 788085-88
E-Mail info@chc-online.de
Internet www.chc-online.de
Marke www.solva.de

Inhaber Dipl.-Oec. Christian Henkel
USt-ID DE 185 162 800

Bankverbindungen
Kasseler Sparkasse (HELADEF1KAS)
IBAN DE11 5205 0353 0002 1205 51
Commerzbank AG (COBADEFF520)
IBAN DE36 5204 0021 0281 1156 00

Anlage 4
Technische und organisatorische Maßnahmen

Das vom Aufragnehmer genutzte Rechenzentrum der Telehouse Deutschland GmbH in Frankfurt/Main ist nach ISO 27001 sowie PCI DSS zertifiziert.

§ 1 Organisationskontrolle

- Datenschutz-Management (Datenschutz-Richtlinie, IT-Sicherheits-Richtlinie, Datenschutz-Verfahrensanweisungen, Incident-Response-Management etc.)
- Verpflichtung der Beschäftigten zur Vertraulichkeit
- Verpflichtung der Beschäftigten auf das Fernmeldegeheimnis
- Verpflichtung von externen Dienstleistern auf das Datengeheimnis, sofern es sich nicht um Auftragsverarbeiter handelt
- Benennung eines Datenschutzbeauftragten
- Regelmäßige Auditierung der technischen und organisatorischen Maßnahmen zum Datenschutz durch den Datenschutzbeauftragten
- Zertifizierung durch IT-Sicherheits- und Datenschutzaudit (PCI DSS)

§ 2 Zutrittskontrolle

Sicherungsmaßnahmen des Gebäudes:

- Bewegungsmelder (Beleuchtung)
- Zu- und Ausgänge des Gebäudes sind von außen nicht zu öffnen
- Sicherung der Fenster, Kellerfenster, Lichtschächte
- Besondere Sicherung der Türen
- Elektronisches Zutrittskontrollsystem für das Gebäude (Magnetstreifen/Speicherchip, RFID-Chip, Codeschloss, biometrisches Verfahren etc.)
- Kartendokumentation
- Schlüsseldokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln

Sicherungsmaßnahmen innerhalb des Gebäudes/der Geschäftsräume:

- Zu- und Ausgänge der Geschäftsräume sind von außen nicht zu öffnen
- Besondere Sicherung der Türen
- Besucherüberwachung (Elektronisches Besuchermanagementsystem, Besucherbuch, Begleitung durch Mitarbeiter etc.)
- Elektronisches Zutrittskontrollsystem für die Geschäftsräume (Magnetstreifen/Speicherchip, RFID-Chip, Codeschloss, biometrisches Verfahren etc.)
- Kartendokumentation
- Schlüsseldokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln

Sicherungsmaßnahmen der besonders sensiblen Räume (Geschäftsleitung, Personalabteilung, IT, Archive, RZ-/Serverraum, TK- Anlage, Verteilerräume, Archive, etc.):

- Zu- und Ausgänge der besonders sensiblen Räume sind von außen nicht zu öffnen
- Besondere Sicherung der Türen
- Closed-Shop-Betrieb
- Elektronisches Zutrittskontrollsystem für besonders sensible Räume (Magnetstreifen/Speicherchip, RFID-Chip, Codeschloss, biometrisches Verfahren etc.)
- Kartendokumentation
- Schlüsseldokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln
- Beaufsichtigte Reinigung und Wartung

§ 3 Zugangskontrolle (Datenverarbeitungsanlagen auf Netz- und Serverebene)

- (Verschlüsselte) Identifikation und Authentifikation von Benutzern (User-ID und Passwort etc.)
- Passwortregeln vorhanden (Mindestlänge, Zeichensatz, Gültigkeitsdauer, Ausschluss Trivialkennworte etc.)
- Vorläufig vergebene Passwörter werden unverzüglich durch sichere Individualpasswörter ersetzt
- Sperrung bei wiederholter Fehleingabe von Passwörtern, Freigabe nur nach Zeitablauf
- Hardware-Firewall vorhanden
- Updates für Firewall werden regelmäßig manuell installiert
- Anti-Virus-Software vorhanden
- Updates für Anti-Virus-Software werden regelmäßig automatisch installiert
- Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei Browsern
- Protokollierung von Internetnutzung
- Sicherheitsmaßnahmen WLAN (Standardeinstellungen, Standardbenutzernamen und Standardpasswörter durch sichere individuelle Einstellungen ersetzt, Verschlüsselungsverfahren, Log-Dateien werden regelmäßig ausgewertet, MAC-Adressfilter aktiviert, regelmäßige Sicherheitschecks etc.)
- Sicherungsmaßnahmen bei Zugang von extern zum Firmennetz (Virtual Private Network (VPN), Protokollierung der externen Kommunikation, regelmäßige Sicherheitschecks von mobilen Endgeräten etc.)

§ 4 Zugriffskontrolle (Datenverarbeitungsanlagen)

- Aktive Netzkomponenten (Switches etc.) sind zugriffssicher untergebracht
- Deaktivierung nicht benötigter Anschlussdosen
- Rollenbasierte Berechtigungen wie Kategorien von Rollen und Rechte der Rollen, insbesondere nach „Lesen, Schreiben, Ausführen“
- Rollen- und Rechtekonzept mit einer Festlegung und Dokumentation der Rollen und Rechte der berechtigten Personen
- Prozess zur Aufhebung nicht mehr benötigter Rollen und Rechte
- Dokumentation der Änderung von Rollen und Rechten
- Regelmäßige Überprüfung der Erforderlichkeit der vergebenen Rollen und Rechte
- Kein Zugriff durch Benutzer auf Systemebene möglich

§ 5 Weitergabekontrolle

- Sensible Daten/Dokumente werden verschlüsselt übertragen
- Regelmäßiges automatisches Einspielen von Sicherheitspatches und/oder -updates bei E-Mail-Programmen
- Protokollierung des E-Mail-Verkehrs und regelmäßige Auswertung auf abweichendes und verdächtiges Mailverhalten
- Geeignete Sicherungsmaßnahmen für den Transport von Datenträgern (Sicherungsbehälter, Sicherung der Daten durch Duplizierung, Verschlüsselung etc.)
- Prozess zur sicheren Löschung/Vernichtung von Datenträgern/Unterlagen (Protokollierung der Vernichtung etc.)
- Einsatz von Aktenvernichtern

§ 6 Eingabekontrolle

- Protokollierung der Einrichtung und des Betriebes von IT-Systemen
- Protokollierung der Einrichtung/Änderung von Benutzern und Rechten (Dokumentation aller berechtigten Nutzer, Rechteprofile der berechtigten Nutzer, Dokumentation von Änderungen von Nutzern/Rechten, Dokumentation, wer die Benutzer und Rechte angeordnet/eingerichtet hat, Historie über die eingerichteten Nutzer und Rechte etc.)
- Protokollierung von Systemänderungen (Dokumentation von funktionalen Systemänderungen/Erweiterungen einschließlich Testfälle, Testung, Testergebnisse und Freigabe, Dokumentation von Versionsänderungen oder Änderungen der technischen Umgebung des IT-Systems, Änderungen der Dateiorganisation oder des Dateiverwaltungssystems etc.)
- Protokollierung von Eingaben und Veränderungen (Datum und Uhrzeit von Zugriffen mit Kennung des Benutzers, Ausgeführte Aktionen, insbesondere Lösch- und Kopiervorgänge, Zugriff auf Dateien mit personenbezogenen oder vertraulichen personenbezogenen Inhalten, unbefugte und abgewiesene Zugriffsversuche, wiederholte Eingabe von fehlerhaften Passwörtern zu einem Login, unbefugtes Einloggen und Überschreiten von Befugnissen, Benutzung von Admin-Accounts, Warnungen über unbefugtes Eindringen etc.)
- Systemüberwachung (Protokollierung von benutzten Programmen, Systemstart und -stopp, Anmeldung/Abmeldung von Benutzern, Anmelde-Fehlversuche, Anschluss und Entfernung von Ein- und Ausgabegeräten, Aktivitäten im Zusammenhang mit Fremdwartung und Fernwartung, Systemwarnungen oder Systemfehler, Konsolwarnungen und Konsolmeldungen, am Paketfilter wegen Regelverstoß abgewiesene Pakete, Änderungen und Änderungsversuche von Gateway- und Firewallpolicies, Systemprotokollausnahmen, Zugriffe auf die Server-Registry, Konfigurations- und Statusänderungen, Systemfehler, Regelverstöße, Maßnahmen zur System- und Datenwiederherstellung, wie Restore- und Back-up-Maßnahmen, Änderungen von Konfigurationseinstellungen etc.)
- Überwachung von Routern und Switches
- Protokollierung von Verbindungs- und Gesprächsdaten
- Protokollierung der Entfernung von Datenträgern
- Protokollierung des Exports, Downloads und Versands von vertraulichen Dokumenten und Daten
- Gewährleistung der Sicherheit von Protokolldateien (Kein Abschalten der Protokollfunktionen möglich, kein Bearbeiten/Löschen der Protokolldateien möglich, Protokollierung der Abschaltung von Protokollfunktionen, Protokollierung der Bearbeitung/Löschung von Protokolldateien, Protokollierung von Zugriffen auf die Protokolldateien, verschlüsselte Speicherung der Protokolldateien etc.)

- Regelmäßige/Anlassbezogene automatische/manuelle Auswertung der Protokolle auf Normabweichungen, Sicherheitsverletzungen und Angriffe

§ 7 Auftragskontrolle

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich des Datenschutzes)
- Vorherige Prüfung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen
- Abschluss eines Vertrages oder eines anderen Rechtsinstruments nach Art. 28 DSGVO und Einhaltung dieser Regularien
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertraglich festgelegte Verantwortlichkeiten
- Sofern Verantwortlicher auch Auftragsverarbeiter ist: Vertragliche Regelungen mit Subunternehmern, dass der Auftraggeber seine Rechte aus AV-Vertrag (insbesondere seine Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann

§ 8 Verfügbarkeitskontrolle

- Ausfallschutz durch gespiegelte Plattenlaufwerke, RAID-System etc.
- Automatisierte Protokollierung der Entfernung von Datenträgern und Auswertung/Prüfung der Protokolle
- Regelmäßige Bestandskontrollen
- Regelmäßige automatisierte Datensicherungen
- Sichere Übertragung von Datensicherungen
- Überprüfung der Sicherungsdaten auf Vollständigkeit und Lesbarkeit
- Überwachung der Sicherungsdatenträger bezüglich ihrer Haltbarkeit/Anzahl der zulässigen Schreibzyklen
- Prüfung der Rekonstruierbarkeit der Datenbestände durch regelmäßige Tests
- Sichere Lagerung von Datensicherungen (anderer Brandabschnitt/externe Lagerung, Tresor, Verschlüsselung der Datensicherungen etc.)
- Unterbrechungsfreie Stromversorgung
- Regelmäßige Tests der unterbrechungsfreien Stromversorgung nach Herstellervorschrift auf Funktionsfähigkeit und Dokumentation der Tests
- Klimaanlage mit Überwachung der Temperatur und des Filterzustands
- Rauchmeldeanlage
- Gasanalysegeräte zur Messung von Feuchtigkeit und Fremdstoffen/Gasen
- Wassermelder
- Brandschutzkonzept
- Brandschutztüren
- Feuerschutzwände
- Brandschutzübungen
- Regelmäßige Überprüfung des räumlichen Umfeldes des RZ/der Serverräume auf eventuelle Risiken (Wasser, erhöhte Brandlast angrenzender Räume etc.) und Dokumentation der Überprüfungen
- Administratorenpasswort/Notfallpassworte sicher hinterlegt (Tresor, Bankschließfach etc.)
- Notfallhandbuch
- Alarmierungsplan

- Wiederanlaufplan

§ 9 Trennungskontrolle

- Logische/physikalische Trennung von verschiedenen speichernden Stellen (Unternehmen)
- Trennung unabhängiger Anwendungen innerhalb eines Unternehmens (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)
- Trennung von Test- und Produktionsdaten (getrennte Programmbibliotheken etc.)
- Trennung der DV-Anlagen und Datenträger für besonders sensible Daten (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)
- Trennung nach Zwecken (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)

CHC ONLINE I SOLVA
Christian Henkel
Friedrich-Ebert-Str. 147
D-34119 Kassel

Telefon +49 561 788085-0
Telefax +49 561 788085-88
E-Mail info@chc-online.de
Internet www.chc-online.de
Marke www.solva.de

Inhaber Dipl.-Oec. Christian Henkel
USt-ID DE 185 162 800

Bankverbindungen
Kasseler Sparkasse (HELADEF1KAS)
IBAN DE11 5205 0353 0002 1205 51
Commerzbank AG (COBADEFF520)
IBAN DE36 5204 0021 0281 1156 00