Sollte das Hosting Ihrer Anwendung von uns durchgeführt werden, führt unser Partner im Rechenzentrum folgende Technische und Organisatorische Maßnahmen durch. Die Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

1. Zweckbindung und Trennbarkeit

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische softwareseitige Mandantentrennung
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern und Signaturen
- pseudonymisierte Daten: Trennung der Zuordnungsdatei und der Aufbewahrung in einem getrennten und abgesicherten IT-System
- Interne Mandantenfähigkeit des Systems
- Funktionstrennung von Produktiv- und Testsystem

2. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

2.1. Verschlüsselung

Die Daten des Auftraggebers werden entsprechend dem Auftrag verschlüsselt.

2.2. Pseudonymisierung

Pseudonymisierung bedeutet, dass die personenbezogenen Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

Es erfolgt eine Pseudonymisierung in folgender Art und Weise:

Personenbezogene Daten werden von Kundenstammdaten, Umsatzdaten strikt getrennt gehalten. Sofern möglich, werden beim elektronischen Transport die personenbezogenen Daten verschlüsselt.

2.3. Zutrittskontrolle

Es werden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

- Alarmanlage
- Kameraüberwachung und Aufzeichnung mit Infrarotsystem
- Automatisches Zugangskontrollsystem mit biometrischen Zugangsdaten über Fingerabdruckleser
- Protokollierung sämtlicher Zu- und Ausgänge
- Unterteilung der Flächen in 3 zutrittsgeschützte Räume
- Zugang erfolgt ausschließlich durch Schleusen
- es ist 24x7 Personal vor Ort anwesend
- abgetrennte und gesicherte Räume für Batterien, USV und Stromversorgung
- Automatisches Zugangskontrollsystem mit Chipkarten

2.4. Zugangskontrolle

Es werden folgende Maßnahmen getroffen, um die Nutzung der Datensysteme durch unbefugte Dritte zu verhindern:

- Zuordnung von Benutzerrechten und Einrichtung eines Benutzerstammsatzes pro Nutzer
- Erstellung von Benutzerprofilen
- differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Passwortvergaben
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Authentifikation mit Benutzernamen und Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie bei Übertragung von Daten
- Sperren externer Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)

- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Einsatz von Intrusion-Detektion-Systemen
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

2.5. Zugriffskontrolle

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

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

- Verschlüsselung von Datenträgern

2.6. Eingabekontrolle

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

2.7. Auftragskontrolle

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

- vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

2.8. Transport- und Weitergabekontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:

- Einsatz von VPN-Tunneln
- Protokollierungssystem

- Schnittstellenanalyse
- Verschlüsselung der Kommunikationswege
- Verschlüsselung physischer Datenträger bei Transport
- Übertragung mit elektronischer Signatur
- Transportsicherung

3. Verfügbarkeit, Wiederherstellung und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- redundante unterbrechungsfreie Stromversorgung (USV), Green-Power USV Systeme von Socomec
- zwei getrennte Stromfeeds durch 2 Unterverteilungen in jedem Rack
- 10kw Stromaufnahme je Rack und mehr möglich
- Notstromversorgung durch 1000kVA Dieselaggregate
- direkter Nachbar des Umspannwerkes
- 3-Stufiger Überspannungsschutz – Grobschutz in Hauptverteilung, Mittel- / Feinschutz in Unterverteilungen, optionaler weiterer Schutz durch kundeneigene Stromanschlussleisten
- VESDA System zur Früherkennung von Rauchentwicklung
- CO2-Feuerlöscher in allen Bereichen sofort griffbereit
- VDS-Alarmanlagen
- direkte Alarmierung des technischen Personals vor Ort sowie externer Mitarbeiter
- Klimatisierung der Serverräume mit einer Mischung aus direkter und indirekter Freikühlung
- Kaltwasserversorgung durch energiesparende Aggregate von Emerson Networks
- Luftaustausch durch Geräte jüngster Generation von Weiss Klimatechnik
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

- Erstellen eines Backup- & Recovery-Konzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- belastbares Datensicherungs- und Wiederherstellungskonzept vorhanden
- Maßnahmen zur Datensicherung (physikalisch / logisch)
- Backup-Verfahren
- Spiegelung von Festplatten mittels Raid-Verfahren
- Einsatz eines Monitoring-Programms
- permanente Überwachung der ordnungsgemäßen Funktionalität
- Einsatz von CWDM Technik für hohe Skalierung der Bandbreiten
- Routing durch moderne Juniper Router
- Coreswitching durch moderne Cisco Switches
- Uplinks wahlweise in 100Mbit, 1GBit oder 10GBit
- Redundante Netzversorgung durch zahlreiche Carrier wie Tiscali International oder die deutsche Telekom
- Peeringverbindungen an diversen Exchangepunkten wie DECiX, AMSiX, KleyReX, ViX und NIX

4. Besondere Datenschutzmaßnahmen

Es liegen schriftlich vor:

- interne Verhaltensregeln
- Risikoanalyse
- Datenschutz-Folgenabschätzung
- Datensicherheitskonzept
- Wiederanlaufkonzept

5. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von einem Jahr und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.