

Anlage B – Datenschutzkonzept / Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

1. Pseudonymisierung: Die Zuordnung von Datensätzen basiert immer auf der Personal- bzw. Kundennummer, nie auf den Rohdatensätzen. Stammdaten sind strikt getrennt gespeichert von anderen Daten (wie bspw. Umsatzdaten)

2. Verschlüsselung: Alle IT-Systeme, die personenbezogene Daten speichern und verarbeiten werden verschlüsselt. Die Verschlüsselung findet auf allen Ebenen (Datenbank, Virtuelle Maschinen etc.) statt.

3. Gewährleistung der Vertraulichkeit: Combi-Connect nutzt die Dienste der Azure Cloud der Microsoft Corporation. Alle Informationen zum Rechenzentrum, Datenschutz und Datensicherheit, sind unter folgender URL beschrieben. <https://www.microsoft.com/de-de/trustcenter>

Alle Firmenrechner sind nur mit Benutzerkennung und Passwort nutzbar. Passwörter entsprechen den gängigen Kennwortrichtlinien. Bei Abwesenheit wird automatisch der Bildschirmschoner aktiv. Zugriff auf Produktionsrelevante Systeme ist nur mit 2 Wege Authentifizierung möglich. Alle Mitarbeiter wurden zu Datenschutzthemen sensibilisiert. Es erfolgt regelmäßige Schulung. Die Verarbeitung von Personenbezogenen Daten unterliegt einem Berechtigungskonzept. Die Rechte sind auf das nötigste Ausmaß reduziert. („Need-to-know- Prinzip“). Es werden die Zugriffe für relevante Informationen protokolliert. Der Umgang mit externen Datenträgern ist in den Unternehmensrichtlinien geregelt. Daten und Dokumente werden ordnungsgemäß entsorgt.

4. Gewährleistung der Integrität: Über Protokoll und Aufzeichnungsmechanismen werden bei personenbezogenen Daten folgende Informationen protokolliert.

- der betroffene Datensatz
- Art der Aktivität
- Zeitpunkt der Aktivität
- der ausführende Nutzer.

5. Gewährleistung der Verfügbarkeit: Combi-Connect nutzt die Dienste der Microsoft Azure Deutschland-Cloud, sowie der Microsoft Corporation. Alle Informationen zum Rechenzentrum, Datenschutz und Datensicherheit, sind unter folgender URL beschrieben. <https://www.microsoft.com/de-de/trustcenter>

6. Gewährleistung der Belastbarkeit der Systeme: Die Belastbarkeit der Systeme wird durch ausreichende Ressourcen und Qualitätsmaßnahmen sichergestellt. Eine Überwachung erfolgt 24/7

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall:

Combi-Connect nutzt die Dienste der Microsoft Azure Deutschland-Cloud, sowie der Microsoft Corporation. Alle Informationen zur Wiederherstellung und Verfügbarkeit, sind unter folgender URL beschrieben. <https://www.microsoft.com/de-de/trustcenter>

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen: Zur Überprüfung der beschriebenen Maßnahmen wurde ein internes Kontrollsystem etabliert. Die Ergebnisse werden regelmäßig geprüft und bewertet.

Es liegen schriftlich vor

- ✓ interne Verhaltensregeln
- ✓ Risikoanalyse
- ✓ allgemeine Datensicherheitsbeschreibung
- ✓ umfassendes Datensicherheitskonzept
- ✓ Wiederanlaufkonzept
- ✓ Zertifikat: ISO/IEC 27001 und des in ISO/IEC 27018:
<https://www.microsoft.com/de-de/TrustCenter/Compliance/ISO-IEC-27001>
<https://www.microsoft.com/de-de/TrustCenter/Compliance/ISO-IEC-27018>

Sonstiges: