Technisch-Organisatorische-Maßnahmen zur Datensicherheit und *Datenschutz*
Art. 5, Art. 30 und Art. 32 DSGVO

Struktur der Firmen-IT
Sensible Bereiche mit Kundendaten sind die 3 PC der ERP-EDV, alle Datensicherungen sowie der Netzwerkserver. Alle dieser Komponenten gestatten nur den Mitarbeitern Zugang, die über die entsprechenden Passwörter verfügen. Eine Datensicherung erfolgt Inhouse auf einem NAS. Eine weitere Datensicherung erfolgt auf Wechselfestplatten, die dann vom GF in seiner Wohnung verschlossen aufbewahrt werden.
Zusätzlich gibt es eine verschlüsselte FTP-Übertragung der Datensicherung auf den Server des Geschäftsführers.

Grundsätze der IT-Sicherheit
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit

Alle gespeicherten Daten sind nach BSI-Standard 100-Z Daten der Kategorie NORMAL.

Vertraulichkeit
- Zugangskontrolle: Die 3 Räume in den die einzig zugriffsberechtigten PCs und der Netzwerkserver stehen sind räumlich getrennt von den übrigen Räumen und werden beim Verlassen verschlossen. Auf diesen 3 PCs läuft das ERP-Programm sowie alle E-mail-Zugänge.
- Zugangsberechtigung: Der Netzwerkserver ist Passwortgeschützt, ein Zugang ist nur als spezieller Nutzer möglich.
- Alle PCs in der Fertigung haben keinen Zugang zum ERP-Programm (weil es nur 3 bezahlte Lizenzen gibt) und auch keine Empfangs-, Einsichts- und Sendemöglichkeit für E-mails.
- Zugangsberechtigung: Alle dieser 3 PCs sind mit benutzerspezifischen Anmeldefunktionen und sicheren Paßwörtern ausgestattet.
- Zugangsberechtigung und Trennungskontrolle: Zugriff auf Buchführung und Lohnabrechnungen ist nur vom Buchführungs-PC aus möglich.
- Alle PCs und der Server werden nach 10 Minuten ohne Eingabe gesperrt (Desktopsperre).
- Eine Besucherregelung bzw. Empfangskontrolle sichert ebenfalls die Vertraulichkeit aller Daten.

Integrität
- Weitergabekontrolle: Lieferanten und andere Dienstleiter erhalten keine Kundendaten.
- Verschlüsselte Verbindung der Kontaktseite der Webseite.
- Bei dem Einsatz von TeamViewer kommt VPN zum Einsatz
- Externe Dienstleister (Wartung und Support des ERP-Programms) erfolgt nur durch einen zuverlässigen Dienstleister; ein ADV-Vertrag ist geschlossen.
- Festplatten sind zur Zeit nicht verschlüsselt.

Verfügbarkeit und Belastbarkeit
- Jeder der PCs verfügt über Firewall und das Betriebssystem Windows10 mit dem Windows Defender oder ein Viren-Abwehrprogramm wie ESET.
- Der Server arbeitet mit Windows2012 und entspricht damit ebenfalls dem Stand der Technik. Die Festplatten sind gespiegelt mit Raid1.
- Ein Brandschutz ist nicht verfügbar. Implementiert ist eine 4-fache Datensicherheit:
  Stufe 1 auf dem Server; gespiegelte Festplatten
  Stufe 2 auf einem in den Werkstatträumen versteckten NAS
  Stufe 3 auf einer an den angeschlossenen Wechselfestplatte, die 1x wöchentlich ausgetauscht und außer Haus gebracht wird
  Stufe 4 ist eine verschlüsselte FTP-Übertragung auf den Server des Geschäftsführers außer Haus.
  Gesichert werden dabei alle Daten, jedoch nicht ein Image des Servers wegen des Dateiumfanges.
  Das Server-Image befindet sich in Stufe 2 und 3.

Kontrolle der Maßnahmen

- Windows10 und Windows7 (noch) gelten zur Zeit als Stand der Technik.
- Betriebssysteme und Anwenderprogramme der Arbeitsplatz-PCs erhalten automatisch Updates
- Der Server wird in 3-monatigen Abständen durch eine IT-Fachkraft aktualisiert

- Verfahrensänderungen werden in den jeweiligen Verfahrensverzeichnissen regelmäßig aktualisiert
- Eine Evaluierung der technisch-organisatorischen-Maßnahmen muss immer stattfinden bei Änderungen der Hard- und Software-Ausstattung
- **Eine Mitarbeiterschulung zu Datenschutz und Datensicherheit findet jährlich statt.**

Verschrottung ausgemusterter Hardware
Programme werden gelöscht
Die Hardware wird ohne Festplatte als gewöhnlicher Elektroschrott entsorgt
Festplatten werden ausgebaut und wie im Bild an einem anderen Gerät gezeigt unbrauchbar gemacht: