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 / Anonymisierung**
   a. Daten, die nur statistischen Zwecken dienen, werden bereits bei der Erhebung so pseudonymisiert oder anonymisiert, dass sie keiner Person zugeordnet werden können.
   b. Daten, die laufend im geschäftlichen Verkehr, z.B. zur Kommunikation, Auftragsbearbeitung, Leistungserbringung und Rechnungsstellung benötigt werden, sind aufgrund ihrer Bestimmung nicht pseudonymisiert.

2. **Verschlüsselung**
   a. **Hosting**
      i. Die Kommunikation mit Internetpräsenzen auf den von uns betriebenen Servern ist grundsätzlich per SSL/TLS verschlüsselt. Jede Internetpräsenz ist standardmäßig mit einem aktuellen Zertifikat einer anerkannten Ausgabestelle versehen.
      ii. Der ausgehende E-Mailverkehr über den SMTP-Server ist zwischen absendendem E-Mailprogramm und unserem Server per SSL/TLS verschlüsselt.
      iii. Der unsere Server verlassende Mailverkehr ist aufgrund technischer Gegebenheiten im Internet nicht zwangsläufig verschlüsselt.
      iv. Wir empfehlen unseren Kunden, eigene Mails mit einem geeigneten Verschlüsselungstool zu sichern.
      v. Kundendaten werden im Shop so verschlüsselt gespeichert, dass sich keine Rückschlüsse auf Personen herstellen lassen.
   b. **Interne Datenverarbeitung**
      i. Intern werden die Daten im laufenden Geschäftsbetrieb unverschlüsselt gespeichert.
      ii. Die datenführenden Systeme sind durch persönliche Zugangskennungen gesichert.
      iii. Zugang zu den Räumen haben nur befugte Personen.

3. **Gewährleistung der Vertraulichkeit**
   a. Alle Mitarbeiter, die mit Daten Dritter in Berührung kommen, sind zur Vertraulichkeit verpflichtet worden.
   b. Die Weitergabe von Daten an Dritte erfolgt ausschließlich zum Zweck der Auftragserfüllung.
   c. Sofern Dritte Daten erhalten, sind diese zur Vertraulichkeit verpflichtet.

4. **Gewährleistung der Integrität**
   a. Die Integrität unserer Mitarbeiter steht außer Frage!

5. **Gewährleistung der Verfügbarkeit**
   a. Die Daten sind jederzeit für Berechtigte verfügbar.
   b. Der Zugriff Dritter, wie z.B. Kontrollbehörden, ist gewährleistet.

6. **Gewährleistung der Belastbarkeit der Systeme**
    a. Sowohl interne wie externe Systeme sind technisch so ausgelegt, dass sie den Anforderungen jederzeit entsprechen und ausreichende Leistungsreserven vorhalten.
    b. Internetserver werden nach spätestens 3 Jahren ausgetauscht, interne Datenserver ca. nach 5 Jahren.

7. **Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall**
    a. Sämtliche Daten sind mindestens doppelt auf verschiedenen Datenträgern gesichert. Die Wiederherstellung ist durch schnelles Rückspielen der Daten jederzeit möglich.

8. **Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen**
    a. Alle technischen Einrichtungen, insbesondere die datenführenden Systeme, werden mindestens einmal wöchentlich auf Funktion und mögliche Fehler geprüft.
    b. Technische Einrichtungen oder Teile davon, welche die ordnungsgemäße Funktion oder Sicherheit nicht vollumfänglich gewährleisten, werden unverzüglich ausgetauscht.
    c. Organisatorische Abläufe werden mindestens einmal pro Jahr vollständig überprüft, bewertet und falls erforderlich angepasst.
    d. Werden im laufenden Betrieb organisatorische Auffälligkeiten festgestellt, werden diese unverzüglich einer eingehenden Prüfung unterzogen und falls erforderlich Anpassungen vorgenommen.

9. **Interne schriftliche Anweisungen und Dokumentationen**
    a. Verhaltensregeln für alle Mitarbeiter
    b. Datensicherheitsbeschreibung
    c. Datensicherheitskonzept
    d. Wiederanlaufkonzept
    e. Notfallanweisungen für Webserver

Stand 25. Mai 2018