Anlage 1

Technische und organisatorische Maßnahmen (TOM)

1. Zugangskontrolle / Zutrittskontrolle

- Gebäude, Datenverarbeitungsanlagen und Räume, in denen Daten verarbeitet werden sind durch Schließsysteme und Alarmanlagen gesichert.
- Zutritt ist nur den berechtigten Personenkreisen gewährt. (Revisionsfähigkeit der Zugangsberechtigung)
- Schlüssel werden personenbezogen vergeben und in den Mitarbeiterstammdaten geführt. Weiterhin besteht ein Zugangskontrollsystem über Pin-Eingabe.
- Der Zugang zu personenbezogenen Daten über Server, Desktop-PCs oder Laptops ist grundsätzlich kennwortgesichert und ebenfalls revisionsfähig.
- Kennwörter werden turnusmäßig geändert.
- Der Zugang ist nur firmenintern möglich.
- Zugänge von ausscheidenden Mitarbeitern werden gesperrt.
- Zugangsregelung und Begleitregelung zum Gebäude für betriebsfremde Personen. Closed Shop-Betrieb nur berechtigte Personen haben Zutritt.

2. Datenträgerkontrolle

- Sämtliche Datenträger mit personenbezogenen Daten mit denen eine aktive Datenverarbeitung stattfindet, befinden sich innerhalb eines verschlossenen Serverschrankes in zusätzlich gesicherten Räumen.
- Mobile Datenträger werden, neben der Archivierung (Aufbewahrung im Tresor), nicht verwendet.

3. Speicherkontrolle

- Nur über Benutzer/Kennwort identifizierte und berechtigte Anwender können personenbezogene Daten speichern oder verarbeiten.
- Bildschirme werden nach längerer Inaktivität des Anwenders abgedunkelt und / oder der Benutzer wird abgemeldet.
- Testsysteme mit geringerer Sicherheitseinstufung sind von Produktiv- / Serversystemen getrennt.
- An-/Abmeldungen an Produktiv- / Serversystemen werden protokolliert.

4. Benutzerkontrolle

- Der Personenkreis mit Berechtigung zu Verarbeitung von personenbezogenen Daten ist klar definiert.
- Die Identifikation an den Datenverarbeitungsanlagen erfolgt durch die Eingabe von Benutzername/Kennwort.
- An-/Abmeldungen an Produktiv- / Serversystemen werden protokolliert.

5. Zugriffskontrolle

- Über serverseitige (zentrale) Berechtigungskonzepte ist sichergestellt, dass Benutzer nur Zugriff auf die für sie freigegeben personenbezogenen Daten erhalten.

6. Übertragungskontrolle

- Externe Zugriffe auf Daten erfolgt über verschlüsselten Verbindungen.
- Sichere Übertragung der Daten im Internet durch SSL-Verschlüsselung (https).

7. Eingabekontrolle

- Die Eingabe von personenbezogenen Daten erfolgt durch den Auftraggeber, Auftragnehmer oder die betroffene Person.
- Bei Auftragseingabe durch den Auftragnehmer werden die Eingabebefugnisse festgelegt.
- Eine Protokollierung (Eingaben und Veränderungen) findet statt.
- Speicherung des Veranlassers

8. Transportkontrolle

- Ein Transport von personenbezogenen Daten findet gemäß der individualisierten Auftragsverarbeitungsverträge (Auftragnehmer / Auftraggeber) nach DS-GVO statt.

9. Wiederherstellbarkeit

- Daten werden regelmäßig auf Sicherungsmedien gesichert und auf Integrität getestet.
- Datenverarbeitungssysteme sind redundant verfügbar bzw. über Fachpersonal in festgelegten Zeiträumen wiederherstellbar.

10. Zuverlässigkeit

- Datenverarbeitungssysteme werden überwacht und regelmäßig gewartet.
- Bei Fehlfunktionen werden die Administratoren informiert.

11. Datenintegrität

- Betriebssysteme und Softwareprogramme erhalten die notwendigen Updates. Virenschutzsoftware ist auf allen Systemen installiert. Firewalls bieten ausreichend Schutz gegen Eindring- und Manipulationsversuche.

12. Auftragskontrolle

- Die Auftragskontrolle ist durch eine klare Vertragsgestaltung / Vereinbarung nach Art. 28 DS-GVO geregelt und die Ausführung entsprechend gewährleistet.
- Kompetenzen und Pflichten sind zwischen Auftraggeber und Auftragnehmer deutlich abgegrenzt.
- Etwaige Unterauftragnehmer sind sorgfältig ausgewählt und auf ihre Aufgaben hingewiesen.
- Mitarbeiter werden auf die sorgfältige, auftragsbezogene Verarbeitung von personenbezogenen Daten hingewiesen und stichprobenartig durch den Datenschutzbeauftragten kontrolliert sowie bei Bedarf regelmäßig nachgeschult.
- Verpflichtung auf die Vertraulichkeit Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO.

13. Verfügbarkeitskontrolle

- Wichtige Daten sind redundant angelegt / gespeichert und innerhalb definierter Reaktionszeiten wiederherstellbar.
- Serveranlagen sind klimatisiert und mit USV (unterbrechungsfreie Stromversorgung) geschützt.
- Es existieren Datensicherungs- und Notfallkonzepte sowie Firewall und Virenschutz.
- Mitarbeiter sind angewiesen Daten auf gesicherten Datenträgern abzulegen.

14. Trennbarkeit

- Personenbezogene Daten werden zweckgebunden verarbeitet.
- Daten aus unterschiedlichen Quellen werden in gesonderten Datenbanken gespeichert.
- Werden Teilmengen von Daten benötigt, werden diese durch geeignete Maßnahmen aus der Gesamtmenge abgefragt.