Zugangskontrolle

» Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie bei der Übertragung von Daten
- Verschlüsselung mobiler Datenträger
- Verschlüsselung der Datensicherungssysteme
- Sperren externer Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall

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 das »Notwendigste« reduziert
- Verschlüsselung von Datenträgern

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:

- 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)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Auftragskontrolle

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

- Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

- schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)

Transport- bzw. 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

3. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

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

- Erstellen eines Backup- & Recoverykonzepts
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Besondere Datenschutzmaßnahmen

» Es liegen schriftlich vor:

- interne Verhaltensregeln

5. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

» Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.