Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DS-GVO der HASOMED GmbH

Inhaltsverzeichnis

1. Zutrittskontrollmaßnahmen

um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- ✓ Alarmanlage mit Anschluss an Sicherheitsdienst
- ✓ Manuelles Schließsystem
- ✓ Videoüberwachung des Hauptzuganges und der Außenbereiche
- ✓ Bewegungsmelder in den Fluren und Sicherheitsbereichen
- ✓ Sicherheitsschlösser an allen Außentüren
- ✓ Personifizierte Schlüsselregelung (Schlüsselausgabe usw.)
- ✓ Firmeninternes Reinigungspersonal
- ✓ Eigener klimatisierter, fensterloser Serverraum

2. Zugangskontrollmaßnahmen

um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- ✓ Automatische Sperrung des Desktops nach fünf Minuten
- ✓ Zuordnung von Benutzerrechten
- ✓ Erstellen von Benutzerprofilen
- ✓ Passwortvergabe
- ✓ Authentifikation mit Benutzername / Passwort
- ✓ Zuordnung von Benutzerprofilen zu IT-Systemen
- ✓ Einsatz von VPN-Technologie
- ✓ Sicherheitsschlösser
- ✓ Personifizierte Schlüsselregelung (Schlüsselausgabe etc.)
- ✓ Firmeninternes Reinigungspersonal
- ✓ Einsatz von Anti-Viren-Software
- ✓ Einsatz einer Software-Firewall
- ✓ Einsatz einer Hardware-Firewall
- ✓ Einsatz von Intrusion-Detection-Systemen

3. Zugriffskontrollmaßnahmen

um die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen zu können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden:

- ✓ Erstellen eines Berechtigungskonzepts
- ✓ Verwaltung der Rechte durch firmeninterne Systemadministratoren
- ✓ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ✓ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel 6-monatlich mit zehn Stellen, Ziffern und Sonderzeichen
- ✓ Sichere Aufbewahrung von Datenträgern
- ✓ Löschung von Datenträgern vor Wiederverwendung
- ✓ Nicht mehr benötigte Papierunterlagen werden geschreddert und dann entsorgt

4. Eingabekontrollmaßnahmen

sodass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht worden sind:

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

5. Auftragskontrollmaßnahmen

sodass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- ✓ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und Verschwiegenheit)
- ✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ✓ Regelmäßige Schulungen der Mitarbeiter zum Thema Datenschutz
- ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

6. Verfügbarkeitskontrollmaßnahmen

sodass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- ✓ Unterbrechungsfreie Stromversorgung (USV)
- ✓ Klimaanlage in Serverräumen
- ✓ Geräte zur Überwachung von Temperatur in Serverräumen
- ✓ Schutzsteckdosenleisten in Serverräumen
- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Erstellen eines Backup- & Recoverykonzepts
- ✓ Testen von Datenwiederherstellung
- ✓ Erstellen eines Notfallplans
- ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ✓ Serverräume befinden sich nicht unterhalb von sanitären Anlagen
- ✓ In Hochwassergebieten: Serverräume über der Wassergrenze

7. Trennungsgebot

Maßnahmen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- ✓ Festlegung von Datenbankrechten
- ✓ Trennung von Produktiv- und Testsystem