

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG
Anlage zur Datenschutzvereinbarung (Wartung und Pflege von IT- und TK-Systemen)

TKS Telekommunikation & Service

Poppenbeck 72,
48329 Havixbeck

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Schlüsselregelung (Schlüsselausgabe etc.)
- Manuelles Schließsystem
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall
- Einsatz einer Hardware-Firewall

3. Zugriffskontrolle

Maßnahmen, 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.

- Erstellen eines Berechtigungskonzepts
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Verwaltung der Rechte durch Systemadministrator
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Einrichtungen von Standleitungen bzw. VPN-Tunneln
E-Mail-Verschlüsselung
Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

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

6. Auftragskontrolle

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

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Schutzsteckdosenleisten in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem

Datum

Helmut Schieve

Verantwortlicher für die Erstellung (in Druckbuchstaben)

Unterschrift des Verantwortlichen