Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

der

GoePaTec GmbH
Adolf-Hoyer-Strasse 3
3,7079 Göttingen

---

1. Zutrittskontrolle

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

- Alarmanlage
- Lichtschranken / Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Wachpersonal
- 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
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Sorgfältige Auswahl von Wachpersonal
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Erstellen von Benutzerprofilen
- Sicherheitsschlösser
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Einsatz einer Software-Firewall
- Sorgfältige Auswahl von Reinigungspersonal
- Verschlüsselung von Datenträgern in Laptops / Notebooks

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
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Verschlüsselung von Datenträgern
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Protokollierung der Vernichtung

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 VPN-Tunneln
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Beim physischen Transport: sichere Transportbehälter/-verpackungen

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.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- 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

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
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Vertragsstrafen bei Verstößen
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeitskontrolle

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

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

8. Trennungsgebot

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

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
-

Göttingen, 04.04.2017
Datum

Carsten Kleine
Verantwortlicher für die Erstellung (in Druckbuchstaben)

Unterschrift des Verantwortlichen