DFAU IDEEN IN ENTWICKLUNG

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

der

DFAU GmbH
Friedrichstr. 4-6
90762 Fürth

Stand des 22. Oktober 2017

Inhaltsverzeichnis

1. Zutrittskontrolle

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

- Schlüsselregelung (Schlüssel- & Chipkartenausgabe)
- Chipkarten-/Transponder-Schließsystem
- Sicherheitsschlösser (Gebäude- und Bürozugang)
- Sorgfältige Auswahl von Reinigungspersonal (Langjährige Festanstellung ohne externe Dienstleister)

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 Reinigungspersonal (Langjährige Festanstellung ohne externe Dienstleister)

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.

- Berechtigungskonzepte für alle Systeme
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

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.

- Verschlüsselung der Datenverbindungen
- Deployment ausschliesslich über nutzergebundene Versionierung und nachvollziehbarer Historie

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.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

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)
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

7. Verfügbarkeitskontrolle

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

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- RAID-Systeme zur Datensicherung

8. Trennungsgebot

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

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

Fürth, 23.10.2017

Ort, Datum

DANIEL FAU

Verantwortlicher für die Erstellung

DFAU Friedrichstr. 4-6 90762 Fürth www.dfau.de

Unterschrift & Stempel