8 TOMs

Technische und organisatorische Schutz-Maßnahmen

Unverzichtbarer Bestandteil des Datenschutzes ist die Datensicherheit. Es müssen geeignete Schutzmaßnahmen auf technischer und organisatorischer Ebene getroffen werden.

Es gibt verschiedene Bereiche, in denen Maßnahmen getroffen werden sollten, um die Verfügbarkeit, Vertraulichkeit und Integrität der Daten zu gewährleisten:

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Bereichen zu verwehren, in denen personenbezogene Daten verarbeitet oder genutzt werden

z.B. durch Einlasskontrolle an den Werkstoren oder den Einsatz eines sicheren Schließsystems

2. Zugangskontrolle

Datenverarbeitungssysteme dürfen nur von befugten Personen genutzt werden können

*z.B. durch individuelle Login-Daten mit sicheren Passwörtern**

3. Zugriffskontrolle

Nur berechtigte Personen dürfen Zugriff auf personenbezogene Daten haben und diese Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

*z.B. Vergabe von differenzierten Benutzerrechten je nach Bedarf für eine bestimmte Tätigkeit**

4. Weitergabekontrolle

Personenbezogene Daten dürfen bei der elektronischen Übertragung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss nachvollziehbar sein, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist oder erfolgt

*z.B. E-Mail-Verschlüsselung, Fernzugriff nur per VPN-Tunnel**

* Hinweis: Eine weitere angemessene Maßnahme ist z.B. eine Verschlüsselung gemäß Stand der Technik. Und wenn ein Notebook, das verloren geht, verschlüsselt war, ist es auch keine meldepflichtige Datenpanne.

8 TOMs
Technische und organisatorische Schutz-Maßnahmen

5. Eingabekontrolle

Die Eingabe, Veränderung und Entfernung von personenbezo-genen Daten in Datenverarbeitungssystemen muss nachvollziehbar sein

z.B. Führen und Kontrollieren von Protokolldateien

6. Auftragskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen

z.B. Abschluss eines aussagekräftigen Vertrages zur Auftragsverarbeitung

7. Verfügbarkeitskontrolle

Personenbezogene Daten müssen wirksam gegen zufällige Zer-störung oder Verlust geschützt werden

z.B. Aufbewahrung der Datensicherung in einem anderen Brandabschnitt, Brandschutzkonzept

8. Trennungsgebot

Daten, die zu unterschiedlichen Zwecken erhoben wurden, müs-sen getrennt voneinander verarbeitet werden

z.B. Kennzeichnung, welche Datensätze zu welchem Kunden gehören, Mandantenfähigkeit von Software

Wenn Sie Fragen zur praktischen Ausgestaltung haben oder sich bezüglich der Angemessenheit einer Maßnahme nicht sicher sind: Fragen Sie Ihren Datenschutzbeauftragten!