

Anwaltsrecht

Technische und organisatorische Maßnahmen der Datensicherheit

DAV-Muster als Checkliste

Art. 32 DSGVO verpflichtet jede Kanzlei zu Maßnahmen, die die Integrität und Vertraulichkeit der Datenverarbeitung gewährleisten. Dieses Muster ist als „Checkliste“ gedacht. Die Punkte, die in diesem Muster genannt sind, sollten mit einem IT-Fachmann besprochen werden. Das Ziel der Besprechung sollte es sein, einen Bericht zu erstellen, der die Maßnahmen dokumentiert, die die Kanzlei zur Datensicherheit ergriffen hat. Sollten sich aus dem Gespräch Vorschläge ergeben zur verbesserten Sicherheit – umso besser. Die Checkliste lautet:

1. Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird.

Zum Beispiel:

- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Abschließbare Serverschränke
- Sorgfältige Auswahl Reinigungspersonal
- Sicherheitsschlösser

2. Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können.

Zum Beispiel:

- Sichere Aufbewahrung von Datenträgern
- Einrichtungen von Standleitungen beziehungsweise VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verschlüsselung von (mobilen) Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern beziehungsweise Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

3. Speicherkontrolle

Die Speicherkontrolle soll verhindern, dass unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können.

Zum Beispiel:

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren

- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passworrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

4. Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können.

Zum Beispiel:

- Festlegung zugangsberechtigter Mitarbeiter
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Regelmäßige Kontrolle von Berechtigungen
- Sperrung von Berechtigungen ausscheidender Mitarbeiter
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von Verschlüsselungs-Technologie
- Einsatz von Anti-Viren-Software

5. Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Zum Beispiel:

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passworrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

6. Übertragungskontrolle

Die Übertragungskontrolle soll gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Zum Beispiel:

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung beziehungsweise vereinbarter Löschfristen

7. Transportkontrolle

Die Transportkontrolle soll gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Zum Beispiel:

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien

8. Wiederherstellbarkeit

Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

Zum Beispiel:

- Erstellen eines Backup- & Recoverykonzepts
- Festplattenspiegelung nach Vereinbarung mit dem Auftraggeber
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans

9. Zuverlässigkeit

Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Zum Beispiel:

- Unabhängig von einander funktionierende Systeme
- Automatisierte Meldung von Fehlfunktionen
- Anti-Viren-Schutz

10. Datenintegrität

Die Datenintegrität soll gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Zum Beispiel:

- Erstellen eines Backup- & Recoverykonzepts

11. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Zum Beispiel: :

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Notfallplans