

Datenschutz und Systemsicherheit

Gesetze kennen!
Regelungen anwenden!

Dipl.-Informatiker Michael Westermann,
Gesundheitsinformatik GmbH, Mannheim

21.04.2005

Gesetze (Auszug)

- Bundesdatenschutzgesetz
- Landesdatenschutzgesetz
- Landeskrankenhausgesetz
- Sozialgesetzbuch I, IV, X
- Röntgenverordnung
- Transfusionsgesetz
- Krebsregistergesetz

Bundesdatenschutzgesetz

Allgemeine und gemeinsame Bestimmungen

- § 1 Zweck und Anwendungsbereich des Gesetzes
- § 2 Öffentliche und nicht öffentliche Stellen
- § 3 Weitere Begriffsbestimmungen
- § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
- § 5 Datengeheimnis
- § 6 Unabdingbare Rechte des Betroffenen
- § 7 Schadensersatz
- § 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen
- § 9 Technische und organisatorische Maßnahmen
- § 10 Einrichtung automatisierter Abrufverfahren
- § 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Datenverarbeitung der öffentlichen Stellen

Rechtsgrundlagen der Datenverarbeitung

- § 12 Anwendungsbereich
- § 13 Datenerhebung
- § 14 Datenspeicherung, -veränderung und -nutzung
- § 15 Datenübermittlung an öffentliche Stellen
- § 16 Datenübermittlung an nicht öffentliche Stellen
- § 17 (weggefallen)
- § 18 Durchführung des Datenschutzes in der Bundesverwaltung

Rechte des Betroffenen

Bundesbeauftragter für den Datenschutz

Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Rechtsgrundlagen der Datenverarbeitung

- § 27 Anwendungsbereich
- § 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke
- § 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung
- § 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form
- § 31 Besondere Zweckbindung
- § 32 (weggefallen)

Rechte des Betroffenen

Aufsichtsbehörde

Sonstige Bestimmungen

- **Sondervorschriften**
- § 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen
- § 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen
- § 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien
- § 42 Datenschutzbeauftragter der Deutschen Welle
- **Schlussvorschriften**
- § 43 Bußgeldvorschriften
- § 44 Strafvorschriften
- **Übergangsvorschriften**
- § 45 Laufende Verwendungen
- § 46 Weitergeltung von Begriffsbestimmungen

Technische und organisatorische Maßnahmen

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungskontrolle

Zutrittskontrolle

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

Zugangskontrolle

- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

Zugriffskontrolle

- zu 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

Weitergabekontrolle

- zu 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 Einrichtung zur Datenübertragung vorgesehen ist

Eingabekontrolle

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

Auftragskontrolle

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

Verfügbarkeitskontrolle

- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

Trennungskontrolle

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