Datenschutz

(das) Recht auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht hat aus Art. 1 und 2 GG das Grundrecht auf **informationelle Selbstbestimmung** abgeleitet.
Das Recht auf **informationelle Selbstbestimmung** beschreibt also das Recht des einzelnen, grundsätzlich selbst zu entscheiden, welche Lebenssachverhalte (Informationen über seine Person und sein Leben) er offenbaren will.

Er hat auch das recht zu erfahren, wer wann wo welche Daten über ihn erfasst oder speichert und das Recht, Daten löschen zu lassen.

Art. 1 GG: Menschenwürde (die Würde des Menschen ist unantastbar)
Art. 2 GG: Persönlichkeitsrechte (freie Entfaltung der Persönlichkeit)

(die) Personenbezogene Daten

Personenbezogene Daten sind **alle Informationen** (Angaben über persönliche oder sachliche Verhältnisse), **die sich auf eine bestimmte** (also bereits identifizierte) oder bestimmbare (mit ein bisschen Recherche identifizierbare) **natürliche** (lebende) **Person beziehen.**
Verschiedene Teilinformationen, die gemeinsam zur Identifizierung einer bestimmten Person führen können, stellen ebenfalls personenbezogene Daten dar.

(die) Gesetzliche Regelungen

Auf der Grundlage einer EU-Richtlinie entstanden **Bundes**datenschutzgesetz und **Landes**datenschutzgesetze.

Mit der **EU-Datenschutz-Grundverordnung (EU-DS-GVO)** ist ein größtenteils einheitliches Datenschutzrecht innerhalb der EU geschaffen worden.

(DIE) VIDEO-ÜBERWACHUNG

Öffentlich zugängliche Räume dürfen durch optisch-elektronische Einrichtungen überwacht werden, soweit diese Maßnahme erforderlich ist…
1. Zur Aufgabenerfüllung öffentlicher Stellen
2. Zur Wahrnehmung des Hausrechts
3. Zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke (z.B. zur Verhinderung von Diebstählen)
Die Tatsache, dass beobachtet wird und wer verantwortlich ist, muss erkennbar gemacht werden.

(die) EU-Datenschutz-Grundverordnung (DSGVO)/ (das) Bundesdatenschutzgesetz

Anwendungsbereiche:
1. Öffentliche Stelle des Bundes
2. Öffentliche Stelle der Länder, sofern der Datenschutz nicht durch Landesgesetze geregelt ist.
3. **Nicht-öffentliche Stellen**: Nicht-öffentliche Stellen können natürliche Personen und juristische Personen des Privatrechts sein.
→ für die automatisierte Verarbeitung personenbezogener Daten
→ für nicht automatisierte Verarbeitung mit einem Datensystem

(die) EU- Datenschutz-Grundverordnung (DSGVO) / (das) Bundesdatenschutzgesetz

Was ist neu?
Rechenschaftspflicht für Unternehmen: Unternehmen müssen nachweisen, dass dem Datenniveau entsprechende Sicherungsmaßnahmen getroffen werden. Wenn diese nicht nachgewiesen werden können, sind Schadenersatzansprüche möglich (allerdings muss dafür ein tatsächlicher Schaden vom Betroffenen nachgewiesen werden).

Grundsätzlich muss eine Risikoanalyse für die Verarbeitung personenbezogener Daten erfolgen.
Die Sicherung personenbezogener Daten muss durch ein spezielles Sicherheitskonzept nachgewiesen werden.
Dazu gehören z.B. Zutrittskontrollen und Videoüberwachung, um den Schutz personenbezogener Daten zu gewährleisten.

Unternehmen müssen alle Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden nach Bekanntwerden der Verletzung der Aufsichtsbehörde melden. → Rechtswidrige Verarbeitung personenbezogener Daten können Straftaten bzw. Ordnungswidrigkeiten sein. Ebenso können Ansprüche auf Ersatz eines Schadens geltend gemacht werden, den der Betroffene jedoch nachweisen muss.

Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist für eine nicht- öffentliche Stelle zu bestellen bei automatisierter Verarbeitung personenbezogener Daten,
wenn:
-in der Regel mindestens 20 Personen ständig hiermit beschäftigt sind
-oder unabhängig von der Anzahl der Mitarbeiter, wenn…
1. Der Verantwortliche oder der Auftraggeber personenbezogene Daten verarbeitet, die der Datenschutz-Folgeabschätzung unterliegen
2. Geschäftsmäßig personenbezogene Daten für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Zu den Aufgaben und Pflichten des Datenschutzbeauftragten gehören:
-die Gestaltung der innerbetrieblichen Organisation des Datenschutz
-die Schulung und Sensibilisierung der Mitarbeiter
-die Überwachung der ordnungsmäßen Anwendung der Datenverarbeitungsprogramme
-die Vorab- Kontrolle sensibler personenbezogener Daten (hierbei handelt es sich um besondere Kategorien personenbezogener Daten, wie z.B. Krankendaten)

Zu diesem Zweck können unterschiedliche Maßnahmen zum Einsatz kommen:
Zutrittskontrolle: um zu gewährleisten, dass Unbefugte der Zutritt zu Datenverarbeitungsanlagen verwehr wird
Zugangskontrolle: hierdurch soll verhindert werden, dass Unbefugte die Datenverarbeitungssystem nutzen können
Zugriffskontrolle: gewährleistet, dass ausschließlich berechtige Person Zugriff auf die Daten erhalten
Trennungskontrolle: personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, müssen getrennt voneinander bearbeitet werden können

Weitere Maßnahmen
Pseudonymisierung: personenbezogene Daten werden verschlüsselt und Identifikationsmerkmale z.B. durch Codes oder Kennzeichen ersetzt (Verwendung der Personalnummer anstelle des Namens)
Weitergabekontrolle: gewährleistet, dass Daten während der Übermittlung nicht unbefugt gelesen, verändert, kopiert oder gespeichert werden können
Eingabekontrolle: dabei wird überprüft wer wann welche Daten eingegeben, verändert oder gespeichert hat
Verfügbarkeitskontrolle: Schutz der personenbezogenen Daten vor Verlust oder Zerstörung