EU-DSGVO: ein wirksamer Schutz der Persönlichkeitsrechte der Bürger?

Vanessa Schadl, h11779184

Präsentation SBWL BIS Kurs 5, 4152,SoSe21, Thema 4

LV-Leiter: ao. Univ. Prof. Dr. Rony G. Flatscher

Inhaltsverzeichnis

1. Einleitung

1.1 Wichtige Begriffsdefinitionen

- Datenverarbeitung – alle Tätigkeiten im Umgang mit Daten (Erhebung, Speicherung, Löschung und Nutzung)
- Verantwortlicher – Person, die über die Datenverarbeitung entscheidet
- Auftragsverarbeiter – Person, die im Auftrag des Verantwortlichen handelt
- natürliche Person – Person mit zuordenbarer Kennung (z.B. Namen) und Träger von Rechten & Pflichten
- juristische Person – Unternehmen mit einer Gesellschaftsform (z.B. GmbH)
- personenbezogene Daten – Informationen zur Identifizierung einer Person (Name, Adresse, Wohnort, usw.)
- sensible Daten – personenbezogene Daten besonderer Kategorie, z.B. Meinungen, Glaubensbekenntnisse

1. Einleitung

1.2 Historische Entwicklung

1970: Hessisches Datenschutz gesetz

1978: DSG 1978 (Ö.)

1980: OECD-Leitsätzen für multinationale Unternehmen (internationale Datenschutzregelung)

1985: Europäische Datenschutzkonvention (international verbindliche Datenschutzregelung)

1995: Richtlinie 95/46/EG (Vorlage für nationale Gesetze der Mitgliedsstaaten; 3 Jahre Zeit)

1999: DSG 2000 (Ö)

2016: EU-DSGVO (Anpassung nationale Gesetze an Verordnung; Bestimmungen bindend)

2018: EU-DSGVO wird wirksam

1. Einleitung

1.3 Motivation der Umsetzung

1. Ursprünglich, wegen Schutz von personenbezogenen Daten als Reaktion auf die zunehmende Automatisierung der Datenverarbeitung

2. Datenschutzrichtlinie 95/46/EG wegen Nichtbeachtung der Datenschutzbestimmungen von den Unternehmen und Digitalisierung
   → Ziel: einheitliche Harmonisierung der Datenschutzrechte innerhalb der Mitgliedsstaaten inklusive Sanktionsmaßnahmen

3. EU-DSGVO wegen Big Data, Industrie 4.0, Robotik und künstliche Intelligenz

   → Riegel für den Datenmissbrauch
   → Einhaltung durch abschreckende Bußgelder

1. Einleitung

1.4 Grundsätze

- Art.5: Grundsätze für die Verarbeitung personenbezogener Daten

✓ **Transparenz**: auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden
✓ **Zweckbindung**: für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden
✓ **Datenminimierung**: dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein
✓ **Richtigkeit**: sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein
✓ **Speicherfrist:** in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist
✓ **Integrität und Vertraulichkeit:** in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet

- Art.6: Verarbeitung nur mit Einverständniserklärung der betroffenen Person
  Ausnahme: unter Anderem, um im Interesse der betroffenen Person zu handeln (Leben retten)

2. Anwendungsbereich

2.1 Sachlicher Anwendungsbereich

Art.2 DSGVO:

- gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen

- gilt ausschließlich zum Schutz von natürlichen Personen und nicht von juristischen Personen

- Ausnahmen:

  Tätigkeiten
  → für die nationale Sicherheit
  → für den privaten oder familiären Gebrauch
  → zur Strafverfolgung und Strafvollstreckung

2. Anwendungsbereich

2.2 Räumlicher Anwendungsbereich

Art.3 DSGVO:

Niederlassung des Verantwortlichen/Auftragsverarbeiters innerhalb EU:

- gilt für alle Unternehmen mit Verarbeitung von personenbezogenen Daten innerhalb oder außerhalb der EU

Niederlassung des Verantwortlichen/Auftragsverarbeiters außerhalb EU:

- gilt bei Verhaltensbeobachtungen und Waren-/ Dienstleistungsangebote, sofern die betroffene Person innerhalb der EU ist (unabhängig, ob die betroffene Person eine Zahlung zu leisten hat)

3. Rechte & Pflichten

3.1 Unternehmen

- juristische Personen haben kein Recht auf Datenschutz, sondern nur Pflichten bei der Datenverarbeitung (in „DSG 2000“ waren sie noch als „Betroffener“ mit erfasst)

3.1.1 Datenverarbeitung

- Einhaltung der Grundsätze (Art.5 DSGVO) und Rechtmäßigkeit der Verarbeitung (Art.6 DSGVO)

- Bestellung internen oder externen Datenschutzbeauftragten wenn,

  → Kerntätigkeit = Verarbeitung von personenbezogenen oder sensiblen Daten
  oder
  → < 9 Personen im Unternehmen verarbeiten personenbezogene Daten

3. Rechte & Pflichten

3.1.2 Verantwortlicher

- natürliche oder juristische Person, die über die Verarbeitung von personenbezogenen Daten entscheidet
- verantwortlich für die Einhaltung der DSGVO-Bestimmungen (haftende Person)

Informationspflicht (Art.13)

- Kommunikation der Verarbeitungsvorgänge direkt zum Zeitpunkt der Datenerhebung
- Übermittlung in einfacher verständlicher Sprache, transparent und auf leicht zugänglichem Wege für die betroffene Person

Verantwortliche?
Zweck?
Daten?
Rechtsgrundlage?
Übermittlung?
Rechte?
Dauer?
Maßnahmen?

3. Rechte & Pflichten

Auskunftspflicht (Art.15)

- Auf Anfrage der betroffenen Person:
  - Auskunft über Datenverarbeitung (unentgeltlich binnen 1 Monat)
  - Umfasst Kopien aller Daten der betroffenen Person
  - Identitätsanalyse um Falschsendungen der Daten zu vermeiden

Mitteilungspflicht (Art.19)

- Nach Veränderung der Daten → Kenntnisnahme aller Empfänger
- Ausnahme: Wenn Mitteilung unzumutbar → Rechtsprechung des Mitgliedsstaates oder Aufsichtsbehörde

Rechenschaftspflicht (Art.5)

- Auf Anfrage der Aufsichtsbehörde:
  - Verantwortlicher muss beweisen, dass er die Datenverarbeitung regelkonform durchführt und die Grundsätze einhält → Hilfestellung durch IT-gestützte Systeme

3. Rechte & Pflichten

Meldepflicht (Art.33)

- Data Breach Meldung innerhalb 72 Stunden an Datenaufsichtsbehörde
  Ausnahme: kein Risiko für Rechte und Freiheiten der Person
- Inhalt: Art der Verletzung, Personenanzahl, Kontaktdaten Verantwortlicher und Datenschutzbeauftragten, Risikobewertung (Auswirkungen, Behebungsmöglichkeiten, Schadenreduzierung)

Dokumentationspflicht (Art.30)

- Verzeichnis aller Verarbeitungstätigkeiten (Wer hat Wie Zugriff auf die Daten)
- Kann von Aufsichtsbehörde verlangt werden
- Ausnahme: < 250 Mitarbeiter **und** eines von den folgenden Kriterien
  - Datenverarbeitung kein Risiko für Rechte und Freiheiten
  - nur gelegentliche Verarbeitung
  - Verarbeitung keiner sensiblen Daten

Recht auf Auftragsverarbeitungsverträge (Art.28)

- Verantwortlicher kann Verträge verfassen, um seine Tätigkeiten oder Pflichten auf einen Auftragsverarbeiter zu verlagern
- Auftragsverarbeiter haftet dann bei einem Verstoß

3. Rechte & Pflichten

3.1.3 Datenschutzbeauftragter

Art.37:

- Bestellung auf freiwilliger Basis
- verpflichtende Bestellung: Kerntätigkeit = Verarbeitung personenbezogener Daten oder bei einer Behörde / öffentliche Stelle
- kann interner Mitarbeiter sein oder externe Stelle
- Überwachung der Einhaltung der DSGVO-Regeln im Betrieb
- Ansprechperson bei Fragen über die DSGVO
- Überprüft ob Verantwortlicher der Meldepflicht nachkommt (Data Breach)
- Zusammenarbeit mit Datenaufsichtsbehörde
- genießt besonderen Kündigungsschutz

3. Rechte & Pflichten

3.2 Betroffene Person

- natürliche Person, von welcher direkt oder indirekt Daten verarbeitet werden
- profitiert von Pflichten der Unternehmen
- Recht auf Ablehnung der Einverständniserklärung

Auskunftsrecht (Art.15)

- Werden personenbezogene Daten verarbeitet? → Falls Ja:
  Auskunft über Zweckbindung, Kategorien, Empfänger, Dauer der Datenverarbeitung
- Nachfragen jederzeit möglich

Berichtigungs- und Löschungsrecht (Art.16 / 17)

- Berichtigungsanfrage jederzeit möglich (bei Nichtberichtigung kann Datenverarbeitung eingeschränkt werden)
- Löschung: bei Widerrufung der Einwilligung, Zweckmäßigkeit nicht mehr erfüllt oder Datenverarbeitung unrechtmäßig

Beschwerderecht

- Bei Vermutung einer Vorschriftsverletzung = jederzeit Beschwerde an zuständige Datenschutzaufsichtsbehörde formlos möglich
- Nach Rechtmäßigkeit der Beschwerde = Schadensersatzzahlungen

4. Sanktionsmaßnahmen

- Aufsichtsbehörde verhängt bei Verstößen Sanktionen an Verantwortlichen/Auftragsverarbeiter
- Ausmaß entscheidet Aufsichtsbehörde und hängt von der Schwere des Vergehens ab
- Schadensersatzzahlungen für betroffene Person (Rest: Entrichtung direkt beim Bund)
- nationale Gesetze können Strafumfang erhöhen (nicht verringern)

Geldbußen

10 Mio. € oder bis zu 2% vom gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres	Pflichtverstoß des Verantwortlichen, Auftragsverarbeiter, Zertifizierungsstelle oder Überwachungsstelle
20 Mio. € oder bis zu 4% vom gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres	Verstoß gegen die Grundsätze, Einwilligungsbedingungen, Rechte der betroffenen Person oder Anweisungen der Aufsichtsbehörde

Beispiele für hohe Geldbußen

Fluggesellschaft „British Airways“: 204,6 Mio. €
Österreichische Post AG: 18 Mio. € → aufgrund Formfehler annulliert (Klage an juristische Person statt natürliche)
Facebook: 5 Mrd. USD

5. Sensible Daten im medizinischen Bereich

5.1 <u>Sensible Daten</u>

personenbezogener Daten besonderer Kategorien:

rassische und ethnische Herkunft, politische Meinungen, Religion und Weltanschauung, Mitgliedschaft in Gewerkschaften, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben bzw. zur sexuellen Orientierung

Art.9: dürfen nicht verarbeitet werden, außer in speziellen Sonderfällen, wenn die Verarbeitung z.B. im Interesse der betroffenen Person liegt (medizinische Hilfe oder Leben retten)

Medizinbereich = viele sensible Daten durch hohe Anzahl der Patienten gegeben

5. Sensible Daten im medizinischen Bereich

5.2 Verarbeitung von Gesundheitsdaten

- Gesundheitsdaten = körperlicher oder geistiger Gesundheitszustand einer Person
- Verarbeitung nur mit Einwilligung des Patienten oder durch eine Zweckbindung → Art.9 Abs.2: lebenswichtiges Interesse, Gesundheitsvorsorge, Arbeitsmedizin medizinische Diagnostik, Versorgung / Behandlung im Gesundheits- oder Sozialbereich + Verwaltung
- Verstöße auch mit Freiheitsstrafen geahndet
- daher organisatorische und technische Maßnahmen notwendig

5.3 Informationssysteme

- IT-gestützte Informationssysteme als technische Hilfe → unterstützen die Sicherheit der Daten und erleichtern Umsetzung der Grundsätze DSGVO
- Erstellung von Patientenarchiv mit Zugriffsteuerung durch ein Berechtigungssystem
- Nachvollziehbarkeit des Zugriffs durch ein Log
- Rechenschaftspflicht professionell gelöst
- Leichte und schnelle Änderung der Daten bei Anfrage der betroffenen Person möglich

5. Sensible Daten im medizinischen Bereich

5.4 Haftung

- niedergelassener Arzt / Ärztin = Verantwortlicher = haftende Person
- mehrere Ärzte in einer Ordination haften generell gemeinsam
- Bei Krankenhäuser haftet die Einrichtung als Ganzes (juristische Person)

5.5 Weitergabe an Dritte

- externe Stellen alltäglich: z. B. Verrechnungen mit Krankenkassen, Anfragen von exekutiven Institutionen, Informationsaustausch mit anderen Krankenhäusern oder Datenaufsichtsbehörde

  ↳ Versendung nur mit Hilfe von verschlüsselten elektronischen Mitteln: herkömmliches Fax oder speziell angefertigte Arztsoftware, wie z. B. „Elda“

- Fragen von Angehörigen alltäglich: Weitergabe der Patientendaten ohne Einwilligung des entsprechenden Patienten ist rechtswidrig und kann sanktioniert werden (bei Volljährigkeit des Patienten)

  ↳ Vorsorge Streitfall: Einwilligungserklärung im Vorhinein abgeben, um in speziellen Fällen problemlos Auskunft zu bekommen

5. Sensible Daten im Medizinbereich

5.6 <u>Aufbewahrungspflicht</u>

- § 51 Abs.3 Ärztegesetz:
  mindestens 10 Jahre Aufbewahrung (Haftungsansprüche 30 Jahre)
- DSGVO - Recht auf Löschung entfällt

5.7 <u>Corona-Pandemie</u>

- Information Gesundheitsamt bei ansteckbare Krankheiten (Masern, Covid 19)
  ↳ öffentliches Interesse und Schutz der nationalen Sicherheit
- Nach Pandemie = Löschung der Daten (Zweckmäßigkeit nicht mehr erfüllt)
- „Grüner Pass“ (Informationen über Corona-Status) wurde abgelehnt

6. Fazit

- Richtiger Schritt in die richtige Richtung für den Datenschutz
- Unternehmen gehen bewusster mit Daten um und setzen Maßnahmen zur Einhaltung der Bestimmungen → Angst vor Geldbuße
- Europa ist Vorbild geworden und inspiriert andere Länder zur Teilnahme
- Schwachpunkte:
    - viele Öffnungsklauseln und Grauzonen in den DSGVO-Bestimmungen
    - E-Commerce: Einverständniserklärung wird durch intransparente Gestaltung der Cookie Verwendung zum Tracking geholt
    - wenig Wissen der Bürger über deren Rechte (Erklärung zu lang oder zu kompliziert)

„Wo kein Kläger, da kein Richter“

Bilderquellen

- https://etailment.de/news/stories/DSGVO-Datenschutz-Datennutzung-EU-Datensilo-Bitkom-Google-Facebook-22298
- https://pixabay.com/de/illustrations/gesetz-symbol-recht-paragraf-447487/
- https://www.sehenswertes-deutschland.de/bundeslaender/reiseinfos-reisetipps-hessen-ferienregionen.html
- https://emojiterra.com/de/rotes-ausrufezeichen/