Vorlesung "Auswirkungen der Informatik"

Datenschutzrecht

Lutz Prechelt
Freie Universität Berlin

- Begründung und Grundlage
- Thesen: Abwägungen, Eiertanz, Zankapfel
- EU-DSGVO
  - und ein wenig BDSG
- sonstiges IT-Recht

Technikgestaltung und Staat

- Der Staat betreibt nicht nur selbst Technikgestaltung
  - z.B. Toll Collect
- sondern setzt auch Regeln fest für die Technikgestaltung der privaten Akteure: Gesetzgebung

Sorten von Gesetzgebung:

- Zivilrecht
  - Verhältnis der Bürger/innen untereinander
  - Wichtigste Quelle: Bürgerliches Gesetzbuch, BGB
- Strafrecht
  - Staat bestraft gemeinschädliches Verhalten
  - Wichtigste Quelle: Strafgesetzbuch, StGB
- Öffentliches Recht
  - Regeln für die staatliche Verwaltung
- (es gibt noch mehr)

- Das Datenschutzrecht enthält Regeln aller drei Sorten
  - hauptsächlich Zivilrecht

Grundregeln demokratischer Rechtsstaaten (konkret: D)

- Staatliche Stellen
  - dürfen nichts, es sei denn, es ist ausdrücklich erlaubt
  - Warum?: Prinzip der *Gesetzmäßigkeit der Verwaltung*:
    - Artikel 20 Grundgesetz: "Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden."
    - → die Details stehen im öffentlichen Recht

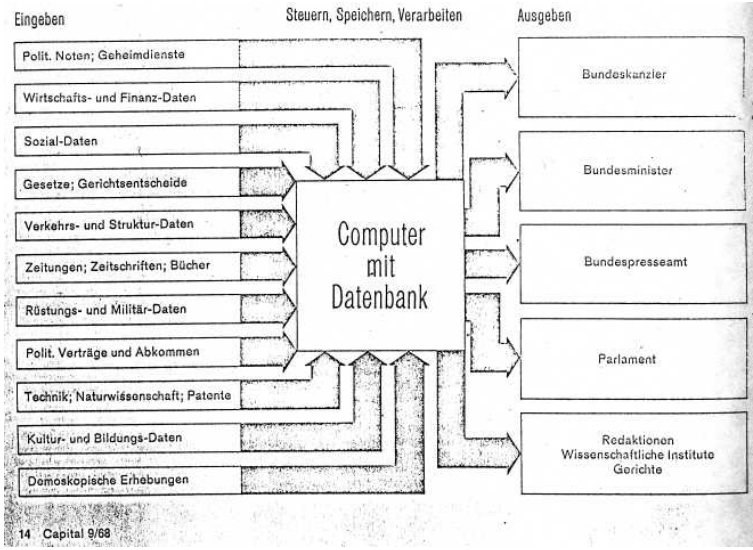
- Privatpersonen (und private Organisationen)
  - dürfen alles, es sei denn, es ist ausdrücklich verboten
  - Warum?: Grundrechte
    - Artikel 1-19 Grundgesetz, z.B. freie Entfaltung der Persönlichkeit
    - → die Details stehen im Zivilrecht und Strafrecht

In Deutschland:

- Seit dem Preußischen Zentralstaat (und auch im 3. Reich) gab es ein zentralisiertes Meldewesen
- 1949: Grundgesetz Artikel 20:
  - (1) Die Bundesrepublik Deutschland ist ein demokratischer und sozialer Bundesstaat.
    - Sozialstaatsprinzip, Bundesstaatsprinzip (Föderalismus)
    - Sozialstaat führt zu starkem Anwachsen der Verwaltungsaufgaben und damit des Informationsbedarfs
    - Föderalismus führt zu Dezentralisierung (z.B.) des Meldewesens
  - (3) Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.
    - Rechtsstaatsprinzip
    - Rechtsstaat verlangt nach gesetzlichen Grundlagen für Regierungs- und Verwaltungshandeln

Kurze Geschichte des Datenschutzes (2)

- Regierungsplan 1968: Bundes-Datenbank-Netz
  - Zusammenführung aller Daten aller Verwaltungen und Erschließung über Personenkennzeichen
  - Kontroverse öffentliche Diskussion
- Einführung erster Datenschutzgesetze in Bundesländern (zuerst 1970 Hessen)
- 1977 erstes Bundes-Datenschutzgesetz (BDSG)
- 1983 Volkszählungsurteil des Bundesverfassungsgerichts
  - **"Recht auf informationelle Selbstbestimmung"**
    - Ein Grundrecht!
- 1990 Neufassung des BDSG
  - "Persönlichkeitsrechtsmodell"
- 2016 EU-Datenschutz-Grundverordnung (EU-DSGVO)
  - gültig seit Mai 2018. Hochkompliziert. War hochumkämpft.



"Datenschutz" ist also ein sehr verkürzender Begriff!

Maßgebliche Grundgesetzartikel

- Artikel 1, Absatz 1:
  "Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

- Artikel 2, Absatz 1:
  "Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

"Volkszählungsurteil" des BVerfG 1983

Aus dem Urteil:

- "*1. [Es] wird der Schutz des Einzelnen gegen unbegrenzte Erhebung […] seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt.*
  Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."
  - Einschränkungen nur verhältnismäßig und im Allgemeininteresse
- "Wer unsicher ist, ob abweichende Verhaltensweisen […] gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."
  - und wäre also unfrei
  - und das wäre schlecht für alle, weil Freiheit für ein demokratisches Gemeinwesen zum Funktionieren wichtig ist.

Thesen

- These "Abwägungen":
  Die informationelle Selbstbestimmung gesetzlich zu regeln erfordert zahlreiche schwierige Abwägungen.

- These "Eiertanz":
  Deshalb enthält das Datenschutzrecht (unvermeidlich) viele schwammige Regeln.

- These "Zankapfel":
  Einige Regeln sind besonders heftig umstritten, weil im Zeitalter von Big Data daran starke Gewinninteressen hängen.

Zankapfel, Eiertanz

Zankapfel: Ein Gegenstand heftigen Streits.

Griechische Mythologie:
καλλίστῃ, "der Schönsten".
Geschenk der Göttin Eris an eine Götterparty, weil sie nicht eingeladen war.

Quelle

Pieter Aertsen:
"Der Eiertanz",
1552

Rechtsquellen

- **EU-Datenschutzgrundverordnung (EU-DSGVO, "EU")**
  - unmittelbar gültig in der gesamten EU
  - recht lang: **99 Artikel** (EU-Infowebsite, Infografik) EU 1, …
  - plus 173 "Erwägungsgründe" als Kommentar
- **Bundes-Datenschutzgesetz (BDSG, "DE")**
  - formt die DSGVO für Deutschland aus
  - auch noch mal lang: **85 Paragraphen** DE 1, DE 2, …
    - viel länger als das alte BDSG, das alles alleine regelte!

- Im Detail saukompliziert!
  - Oft kann man Gesetze ganz gut auch als Laie lesen. Diese hier eher schwer. **Wir betrachten sie nur sehr grob!**
    - *Für echte Anwendungen unbedingt direkt im Rechtstext nachlesen*
- Gute Netzquelle: **dsgvo-gesetz.de**
  - verbindet EU-DSGVO-Artikel mit zugehörigen Erwägungsgründen und BDSG-Paragraphen

Jetzt wird's trocken!

- Es gibt 11 Kapitel in der DSGVO

- Gilt für: Behörden, Firmen, Vereine etc. (EU Art. 2,3, DE §1, also in unserer Notation: EU 2, EU 3, DE 1)
  - Inkl. Außer-EU-Firmen, die in der EU Waren/Dienstleistungen anbieten (auch unentgeltliche).
  - Div. Einschränkungen in anderen Gesetzen, insbes. für Geheimdienste
  - Nicht gültig im rein privaten Bereich
- Deckt ab: Alle Verarbeitung "personenbezogener Daten"

- 25 Begriffsbestimmungen in EU 4, plus 4 in DE 2
  - z.B. personenbezogene Daten, betroffene Person, Verarbeitung, Profiling, Verantwortlicher (**V**), Auftragsverarbeiter (AV), Empfänger, Einwilligung; öffentliche/nichtöffentliche Stelle.
  - Für genaue Bedeutung wichtig; wir gehen damit eher lässig um

Anforderungen:

- a) rechtmäßig, transparent
- b) Zweck eindeutig festgelegt und legitim
  - "Zweckbindung"
- c) zweckangemessen, auf zwecknötiges Maß beschränkt
  - "Datenminimierung" (altes BDSG: "Datensparsamkeit")
- d) Daten korrekt und aktuell
  - Maßnahmen zur ggf. Berichtigung oder Löschung
- e) Speicherung nur so lange, wie für Zweck nötig
- f) Schutz der Daten vor unrechtmäßiger Verarbtg., vor Verlust/Zerstörung/ Verfälschung

Rechtmäßigkeit der Verarbeitung (EU 6)

(1) Nur gegeben, wenn:

- a) **Einwilligung** vorliegt,
- b) zur Vertragserfüllung,
- c) wg. rechtlicher Verpflichtung,
- d) zum Schutz lebenswichtiger Interessen,
- e) im öffentl. Interesse oder für staatliche Aufgabe,
- f) zur Wahrung berechtigter Interessen
  - aber abgewogen gegen Interessen Betroffener.

(Einwilligung bietet die größte Rechtssicherheit)

Rechtmäßigkeit der Verarbeitung (DE)

- DE 3: Verarbeitung durch **öffentliche** Stellen
  - nur zur Aufgabenerfüllung
- DE 23: Verarbeitung zu anderen Zwecken durch öffentliche Stellen
  - nur aus 6 benannten Gründen, z.B. Verfolgung v. Straftaten
- DE 24: Verarb. zu and. Zw. durch **nichtöffentliche** Stellen
  - nur f. Gefahrenabwehr und zivilrechtliche Ansprüche
- DE 25: Datenübermittlungen durch öff. Stellen
  - an öff. St.: nur wenn nötig, gleiche Zweckbindung
  - an nichtöff.: auch bei berecht. Interesse; zweckgebunden

Ferner:

- DE 4: Videoüberwachung öffentlich zugänglicher Räume
  - nur f. berecht. Interessen
- DE 27: Datenverarb. zu wissensch./histor. Forschgs-zwecken u. statist. Zwecken
  - abgewog. Sondererlaubnisse
- DE 31: Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften
  - Bonitäts-Scoring nur m. Einschränkungen erlaubt

Bedingungen für die Einwilligung (EU 7, 8)

- (2) Einwilligung darf nur wenig mit anderen Dingen vermischt werden
- (3) Einwilligung kann jederzeit widerrufen werden
  - das muss man vor der Einwilligung auch erläutern
  - es darf nicht schwieriger sein als die Einwilligung
  - wirkt nur in die Zukunft
- (4) Einwilligung darf zur Vertragserfüllung nur im nötigen Ausmaß verlangt werden

- EU 8: (1) Für Kinder unter 16 müssen die Eltern einwilligen
  - (2) und der V. muss sich angemessen darum bemühen, dass das wirklich die Eltern waren.

Verarbeitung besonderer Kategorien personenbezogener Daten (EU 9)

Freie Universität Berlin

- (1) Verboten ist Verarb. von Daten zu:
  - rassische/ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische ID-Daten, Gesundheit, Sexualleben, sexuelle Orientierung
- (2) Ausnahmen:
  - a) nach **Einwilligung**
  - b) wg. Arbeitsrecht oder Sozialschutz
  - c) wg. lebenswichtiger Interessen
  - d) "passende" Verarb. durch einschlägige Organisation
    - z.B. Gewerkschaft oder Kirche darf ihre Mitglieder kennen
  - e) Daten sind vom Betroffenen öffentlich gemacht
  - f) wg. Rechtsansprüchen oder durch Gericht
  - g) angemessen im öff. Interesse mit besond. Rechtsgrundlage
  - h) medizinischer Bereich, (i) öffentl. Gesundheit
  - j) angemessen u. besonders geschützt f. Forschung/Statistik

DE 22 schärft das nach

Sonstige Grundsätze (EU 10, 11)

- Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (EU 10)
  - nur unter behördlicher Aufsicht oder m. besond. Rechtsgrundlage

- Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist (EU 11)
  - Ist der Personenbezug nicht (mehr) nötig, darf der V. ihn löschen
    - und EU 15 bis EU 20 werden dann nicht angewendet
  - und soll das ggf. Betroffenen mitteilen.

Kapitel 3: Rechte Betroffener:
Auskunft (EU 12-14)

Freie Universität Berlin

- EU 12: V. muss über Auskunftsrechte EU 13-22 in verständlicher Form informieren
  - und mit einfachen Verfahren, binnen 1 Monat, meist unentgeltlich Auskunft geben.
- EU 13: Bei Erhebung muss vom V. mitgeteilt (oder (4) vorher zugänglich gemacht) werden:
  - (1) a) Kontaktdaten d. Verantwortlichen, c) Zwecke, d) ggf. die berechtigten Interessen, e),f) ggf. Empfänger
  - (2) a) Dauer d. Speicherung, b) c) d) Rechte des Betroffenen, f) ggf. Logik u. Wirkungen automatisierter Entscheidungsfindung
- EU 14: (1) (2) Ähnlich auch, wenn nicht bei Betroffenen erhoben
  - (3) und zwar zügig
  - (5) außer wenn a) schon bekannt, b) Aufwand unverhältnismäßig oder d) Vertraulichkeitspflicht besteht

Auskunftsrecht der betroffenen Person (EU 15)

- (1) Man kann Auskunft verlangen über:
  - a) Zwecke b) Kategorien verarbeiteter Daten
  - c) Empfänger d) geplante Dauer der Speicherung
  - g) Herkunft der Daten
  - h) ggf. Logik & Wirkungen automatischer Entscheidungsfindung

- (3) "Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung."
  - und zwar "in einem gängigen elektronischen Format", wenn der Antrag elektronisch war.

Recht auf Berichtigung (EU 16, 19), Recht auf Löschung (EU 17, 18, 19),

Freie Universität Berlin

- EU 16: Sind Daten unrichtig, kann man unverzügliche Berichtigung oder Vervollständigung verlangen.
- EU 17:
  - (1) Man kann Löschung verlangen, wenn
    - a) Daten nicht mehr notwendig
    - b) Einwilligung wird widerrufen c) Widerspruch wird eingelegt
    - d) Verarbeitung war unrechtmäßig
  - (2) Bei öffentlich gemachten Daten muss V. angemessen die Welt über das Löschverlangen informieren
  - (3) Beides nicht, falls Verarbeitung nötig für:
    - a) Recht auf Meinungsäußerung und Information
    - b) c) d) e) rechtl. Verpflichtung, öffentl. Interesse, Rechtsansprüche
- EU 18:
  - Statt Löschung kann man oft auch Sperrung verlangen
    - insbes. während Richtigkeit oder Rechte geklärt werden
- EU 19: Berichtigung/Löschung ist Empfängern mitzuteilen

Recht auf Datenübertragbarkeit (EU 20) Widerspruch (EU 21)

- EU 20: (1) "Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem V. bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten […]"
- (2) "[und das Recht,] dass die personenbez. Daten direkt von einem V. einem anderen V. übermittelt werden, soweit dies technisch machbar ist"

- EU 21: (1) Einer erlaubten Verarbeitung, die ohne Einwilligung erfolgt, kann man aus besonderer eigener Situation heraus widersprechen.
  - Nicht gegen zwingende schutzwürdige Gründe des V.
  - (2) (3) Immer bei Direktwerbung
  - (5) Manchmal auch mittels automatisierter Verfahren (z.B. do-not-track)

Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (EU 22)

- (1) Komplett automatisierte Entscheidungen sind nicht erlaubt, wenn sie betroffene erheblich beeinträchtigen, außer:
  - (2) a) wenn für Vertragserfüllung nötig
  - b) wenn nach Rechtsvorschrift erlaubt
  - c) wenn Einwilligung vorliegt
- (4) besondere Kategorien personenbez. Daten sind noch starker eingeschränkt.

Beschränkungen der Rechte (EU 23)

- (1) Die Rechte nach EU 12-22 können für wenige Zwecke beschränkt werden (wenn demokratisch u. verhältnismäßig):
  - a) nationale Sicherheit b) Landesverteidigung
  - c) öffentl. Sicherheit d) g) h) Strafverfolgung u.ä.
  - e) sonstige allg. öff. Interessen
  - f) Unabhängigkeit der Justiz
  - i) Schutz der Rechte von Personen
  - j) Durchsetzg. zivilrechtlicher Ansprüche

- (2) Die beschränkenden Regeln müssen zahlreiche Bedingungen erfüllen (a bis h)

Kapitel 4: Verantwortlicher u. Auftragsverarbeiter
EU 24, 25, 26, 27

- EU 24: Verantwortlicher (V) muss Vorkehrungen zur Regeleinhaltung treffen und das nachweisen können
- EU 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
  - Pseudonymisierung wo möglich, Datenminimierung, Speicherfristen, per Voreinst. nur nötige Daten f. Zweck, Zugang nur f. beschränkten Personenkreis

- EU 26: Gemeinsam für die Verarbeitung Verantwortliche legen angemessen fest, wer welchen Teil der Pflichten übernimmt und teilen das mit
  - Betroffene können Rechte bei allen geltend machen
- EU 27: Außer-EU-V. müssen Inner-EU-Vertreter benennen.

EU 28:

- (1) Nur verlässliche Auftragsverarbeiter (AV) sind erlaubt
- (2) Die dürfen weitere AV nur nach Genehmigung beauftragen
- (3) Sie müssen vertraglich an die DSGVO und weitere spezifische Pflichten a) bis h) gebunden werden
- (4) und müssen diese ggf. an weitere AV weitergeben

EU 30:

- (1) V. und Vertreter führen Verzeichnis von Verarb.tätigk.: zust. Personen, Zwecke, Kateg. betroffener Personen, Kateg. von Empfängern, Übermittlungen in Drittländer, Löschfristen, organis. Maßnahmen
- (2) ähnlich die AV
- (5) Ausnahmen manchmal für V. unter 250 Mitarbeitern

Sicherheit der Verarbeitung (EU 32)
Meldung von Datenschutzverletzg. (EU 33, 34)

- EU 32: (1) Verarb. muss nach Stand der Technik erfolgen, mit Maßnahmen zur Risikosenkung wie
  - a) Pseudonymisierung, Verschlüsselung
  - b) dauerhafte Fähigkeit, Vertraulichk., Integrität u. Verfügbark. sicherzustellen
  - c) funktionierendes Backup/Restore
  - d) Verfahren zur Überwachung der Wirksamkeit der Maßnahmen
- (2) Vorbeugung muss verhältnismäßig zum Risiko erfolgen

- EU 33: (1) V. melden DS-Verletzungen binnen 72h an Aufsichtsbehörde; (2) AV melden an V.
  - (3) Meldung enthält mindestens: Betroffene, Kontaktperson, vermutliche Folgen, ergriffene Maßnahmen
- EU 34: Bei relevanten Verletz. muss auch der Betroffene benachrichtigt werden
  - (3) c) oder ggf. öffentliche Bekanntmachung

Datenschutz-Folgenabschätzung (EU 35, 36)

- EU 35: (1) (3) In riskanten Fällen muss V. eine Technikfolgenabschätzung aufschreiben:
  - (7) a) Verarbeitungsvorgänge
  - b) Bewertung Notwendigkeit und Verhältnismäßigkeit
  - c) Bewertung Risiken für Betroffene
  - d) geplante Abhilfemaßnahmen
- EU 36: (1) (3) V. muss Aufsichtsbehörde konsultieren, wenn demnach hohes Risiko besteht
  - (2) Diese kann dann Empfehlungen geben
- EU 36: (4) Mitgliedstaaten konsultieren Aufsichtsbehörde bei der Vorbereitung von Datenschutz-Gesetzgebung

Datenschutzbeauftragte (EU 37, DE 38, EU 38)

- DE 38: Die meisten Organisationen brauchen eine/n Datenschutzbeauftragte/n (DSB)
  - insbes. immer ab 10 verarbeitenden Personen
- EU 37: (5) DSB muss qualifiziert sein
- EU 37: (2) (3) (4) aber mehrere Organisationen können sich DSB teilen
- EU 38: (1) DSB muss eingebunden werden,
  (2) muss Unterstützung, Ressourcen und Zugang erhalten,
  (3) darf als DSB keine Weisungen erhalten und nicht einfach abberufen werden
  - (4) Betroffene können DSB konsultieren
  - (5) DSB hat Vertraulichkeitspflicht
- EU 39: DSB unterrichtet V. über Pflichten und überwacht deren Einhaltung

Verhaltensregeln (EU 40, 41)
Zertifizierung (EU 42, EU 43)

Freie Universität Berlin

- EU 40: (5) Verbände u.ä. können Durchführungs-Verhaltensregeln formulieren
  - (5) die von der Aufsichtsbehörde genehmigt und veröffentlicht werden
  - (7) (8) (9) (10) (11) diese können ggf. sogar von EU-Gremien EU-weit verbindlich gemacht werden

- EU 41: Deren Überwachung kann von der Aufsichtsbehörde einer eigens dafür akkreditierten Einrichtung übertragen werden.

- EU 42: (1) Es sollen Zertifikate/Siegel eingeführt werden, die die Einhaltung der DSGVO bescheinigen
  - (2) auch (per vertraglicher Bindung) für Außer-EU-V. und AV.
- EU 43: Dafür werden Zertifizierungsstellen akkreditiert

Kapitel 5: Datenübermittlung an Drittländer
EU 44, 45, 48, 49

- EU 44: Außer-EU-Übermittlung ist nur erlaubt, wenn Einhaltung der DSGVO weiter gewährleistet werden kann
  - EU 46: (1) (2) (3) (4) (5) Details dazu, wie das aussehen kann
- EU 45: (1) Ist pauschal erlaubt, wenn die EU für das Drittland "angemessenes Schutzniveau" festgestellt hat
  - (2) (3) (4) (5) (6) (7) (8) (9) Regeln dazu, wie das geht.
- EU 48: V. dürfen aufgrund von Außer-EU-Gerichts- oder -Verwaltungsanforderungen Daten nur übermitteln, wenn Rechtshilfeabkommen besteht
  - ((ein spannendes Gerangel zwischen EU und USA))
- EU 49: Liste von Ausnahmeerlaubnissen f. Übermittlung in Drittländer
  - z.B. Einwilligung der Betroffenen, Interessen der Betroffenen

Datenübermittlung innerhalb von Konzernen (EU 47)

- EU 47: Internationale Firmengruppen können sich länderübergreifende DSGVO-konforme Regeln geben
  - Aufsichtsbehörde genehmigt die ggf. nach Anforderungen (1) a) b) c), (2) a) b) c) d) e) f) g) h) i) j) k) l) m) n)

Kapitel 6: Unabhängige Aufsichtsbehörden
EU 51-59

Freie Universität Berlin

- EU 51: Jeder EU-Staat richtet Aufsichtsbehörde(n) (AB) ein
  - EU 52: (1) (2) (3) (4) (5) (6) AB sind unabhängig
  - EU 53: (1) Mitglieder müssen in transparentem Verfahren ernannt werden (→EU 54), (2) qualifiziert sein, (4) dürfen nur unter wenigen Umständen enthoben werden
  - DE 12, DE 13: Detailregeln für Deutschland
- EU 57: (1) Aufgaben:
  - a) Verordnung durchsetzen
  - b) Öffentlichkeit aufklären, insbes. Kinder
  - c) Parlament, Regierung, Einrichtungen beraten
  - d) V. und AV sensibilisieren
  - sowie ferner e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v)
- EU 58: AB hat entsprechende Befugnisse
  - Siehe auch DE 16, 21, 29, 40
- EU 59: AB erstattet jährlich öffentlich dem Parlament Bericht

- Darin geht es um die Zusammenarbeit der AB der Staaten und mit der EU, um ein sinnvoll zusammenpassendes ("kohärentes") Gesamtregime hinzubekommen.
  - DE 18: In Deutschland gibt es zudem noch Länder-Datenschutzbehörden

Kapitel 8: Rechtsbehelfe, Haftung und Sanktionen
(EU 77-84)

- EU 77 Recht auf Beschwerde bei einer Aufsichtsbehörde
- EU 78 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde
- EU 79 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter
- EU 80 Vertretung von betroffenen Personen
- EU 81 Aussetzung des Verfahrens
- EU 82 Haftung und Recht auf Schadenersatz
- EU 83 Allgemeine Bedingungen für die Verhängung von Geldbußen
- EU 84 Sanktionen

Zusammen:

- Rechtsschutz
  - auch gegen außer-EU-V. (wg. EU 27),
  - auch durch NGOs wahrnehmbar (EU 80)

Schadenersatz und Geldbußen (EU 82, EU 83, DE 41, DE 43)

- EU 82: (1) Schadenersatz für DSGVO-Verletzung steht ggf. Geschädigten zu, selbst wenn sie nicht Betroffene sind.
- EU 83: (1) Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein.
  - (2) Zu berücksichtigen sind a) b) c) d) e) f) g) h) i) j) k).
  - (4) Höhe in best. Fällen a) b) c) bis 2% d. **weltweiten** Jahresumsatzes (mind. bis 10 Mio. EUR)
  - (5) (6) in anderen Fällen a) b) c) d) e) sogar bis 4%
  - (sogar Google zittert vor dieser Regel)
- DE 41: Es findet dabei das Ordnungswidrigkeitenrecht und Strafrecht Anwendung
- DE 43: (3) Gegen öffentliche Stellen werden keine Geldbußen verhängt

Kapitel 9: Vorschriften für besondere Verarbeitungssituationen (EU 85-91)

Freie Universität Berlin

- EU 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit
  - zu harmonisieren. Z.B. (2) Wissenschaft und Journalismus bekommen nötigenfalls Sonderrechte
- EU 86 Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten
- EU 87 Verarbeitung der nationalen Kennziffer
- EU 88 Datenverarbeitung im Beschäftigungskontext
- EU 89 Garantien/Ausnahmen bei Verarbeitung zu im öffentlichen Interesse liegenden Archiv-/wiss./stat. Zwecken
  - bekommen Sonderrechte, aber: Datenminimierung, Pseudonymisierung verlangt
- EU 90 Geheimhaltungspflichten
- EU 91 Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

Kapitel 10:

- EU 92 Ausübung der Befugnisübertragung
- EU 93 Ausschussverfahren

Kapitel 11:

- EU 94 Aufhebung der Richtlinie 95/46/EG
- EU 95 Verhältnis zur Richtlinie 2002/58/EG
- EU 96 Verhältnis zu bereits geschlossenen Übereinkünften
- EU 97 Berichte der Kommission
- EU 98 Überprüfung anderer Rechtsakte der Union zum Datenschutz
- EU 99 Inkrafttreten und Anwendung

Puh!

Thesen

- These "Abwägungen":
  Die informationelle Selbstbestimmung gesetzlich zu Regeln erfordert zahlreiche schwierige Abwägungen.

- These "Eiertanz":
  Deshalb enthält das Bundesdatenschutzgesetz (unvermeidlich) viele schwammige Regeln.

- These "Zankapfel":
  Einige Regeln sind besonders heftig umstritten, weil im Zeitalter von Big Data daran starke Gewinninteressen hängen.

Hilfen zur Anwendung

- EU-Informationsseiten
  - für Bürger/innen
  - für Unternehmen etc.
- Die Artikel-29-Datenschutzgruppe der EU veröffentlicht "Guidelines"
  - z.B. zur Zustimmung
- Datenschutzkonferenz (DS-Behörden von Bund und Ländern) veröffentlicht "Kurzpapiere" zu diversen Teilthemen

Datenschutz-Beauftragte

- Bundesbeauftragte für den Datenschutz
  - Ulrich Kelber
  - http://www.bfd.bund.de
- Berliner Beauftragte für Datenschutz und Informationsfreiheit
  - Maja Smoltczyk
  - http://www.datenschutz-berlin.de/
- Virtuelles Datenschutzbüro
  - https://www.datenschutz.de/
  - z.B. Katalog von Datenschutzrecht

Ulrich Kelber

Maja Smoltczyk

Ein duales Konzept: Informationsfreiheit

- Recht der Bürger auf Zugang zu den Informationen, die in öffentlichen Stellen vorliegen
  - Bürgerrecht in Schweden seit 1766
  - UNO 1946: "a fundamental human right"
  - In vielen Ländern seit langem gesetzlich verankert z.B. seit 1966 in den USA (Freedom of Information Act)
  - Auch für die Organe der EU
    - http://www.informationsfreiheit.de/info_eu/index.htm
    - und in vielen europäischen Ländern
  - Deutschland: Informationsfreiheitsgesetz (2006)
    - auch einige Länder inkl. Berlin und Brandenburg
- Duales Gegenstück zum Datenschutz
  - Datenschutz: Abwehrrecht des Individuums
  - Informationsfreiheit: Leistungspflicht des Staates

Andere wichtige Quellen von IT-Recht

- Zivilrecht
  - z.B. Persönlichkeitsrecht (relevant z.B. für Fotos von Menschen)
  - z.B. Vertragsrecht, Haftung/Schadenersatz, Störerhaftung, Gewährleistung
- Urheberrecht
  - relevant für das Nutzen (z.B. "Teilen") von Bildern, Videos, Musik, Texten, etc.
- Telemediengesetz (und anderes Medienrecht)
  - z.B. Impressum, Spam, gesetzeswidrige Inhalte, Datenschutz, Providerprivileg
- Telekommunikationsrecht
  - wichtig für Betreiber, bis hin zur Vorratsdatenspeicherung

- u.a.

Zusammenfassung

- Das Datenschutzrecht beschreibt, in welchen Fällen und wie personenbezogene Daten verarbeitet werden dürfen
- Grundideen sind die Datensparsamkeit und die informationelle Selbstbestimmung
- Die meisten Regeln folgen diesen Grundideen und sind deshalb recht restriktiv (➔ Zank)
  - Sie kennen jedoch viele Ausnahmen und Abwägungsklauseln (= Eiertanz)
- Beste Grundlage für eine legale Verwendung von Daten ist meist eine ausdrückliche Einwilligung unter Nennung des Zwecks
- Viele andere Rechtsvorschriften müssen ebenfalls beachtet werden

Danke!