Karlsruher Institut für Technologie

Datenschutz und Privatheit in vernetzten Informationssystemen

Kapitel 7: Datenschutz und Recht

Erik Buchmann (buchmann@kit.edu)

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“

Inhalte und Lernziele dieses Kapitels

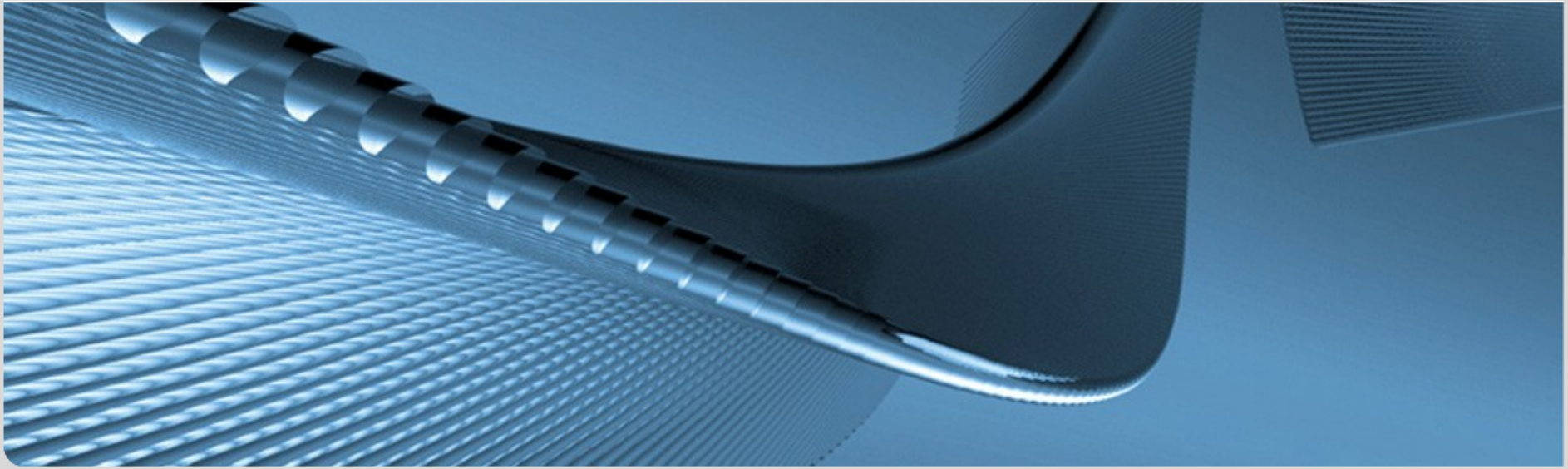
- Einführung
- Datenschutz International
- Datenschutz Deutschland
  - Bundesdatenschutzgesetz
  - Telemediengesetz
- Vorratsdatenspeicherung
- Abschluss

- Lernziele
  - Sie können erklären, wie der deutsche Datenschutz im internationalen Rahmen verankert ist.
  - Sie können einen Überblick darüber geben, welche fundamentalen gesetzlichen Normen bestehen, und in welchen Gesetzen sie zu finden sind.
  - Sie können diese Normen auf einfache Vorfälle anwenden.

Karlsruher Institut für Technologie

Einführung

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



Deutschlands größte Datensammler

Datensammler	Betroffene	Attribute
Schufa	64 Mio.	Name, Geburtsdatum, Adresse, Girokonten, Kreditkarten, Kredite, etc.
Creditreform Consumer	22 Mio.	
Infoscore	7.7 Mio.	
Global Group	65 Mio.	Konsumverhalten nach Regionen aufgeschlüsselt, sozialdemografische Daten, Freizeitverhalten
AZ-Direct (Bertelsmann)	70 Mio.	
Schober Informations Group	50 Mio.	
Saf Solutions	32 Mio.	Inkasso-Unternehmen, Abrechnungsdaten
HIS (Datenbank der großen Versicherungen)	9.5 Mio.	Versicherungsdaten, KFZ-Schäden, Anspruchsteller

Quelle: www.spiegel.de, 12/2008

Prinzipien des Datenschutzes

Wiederholung

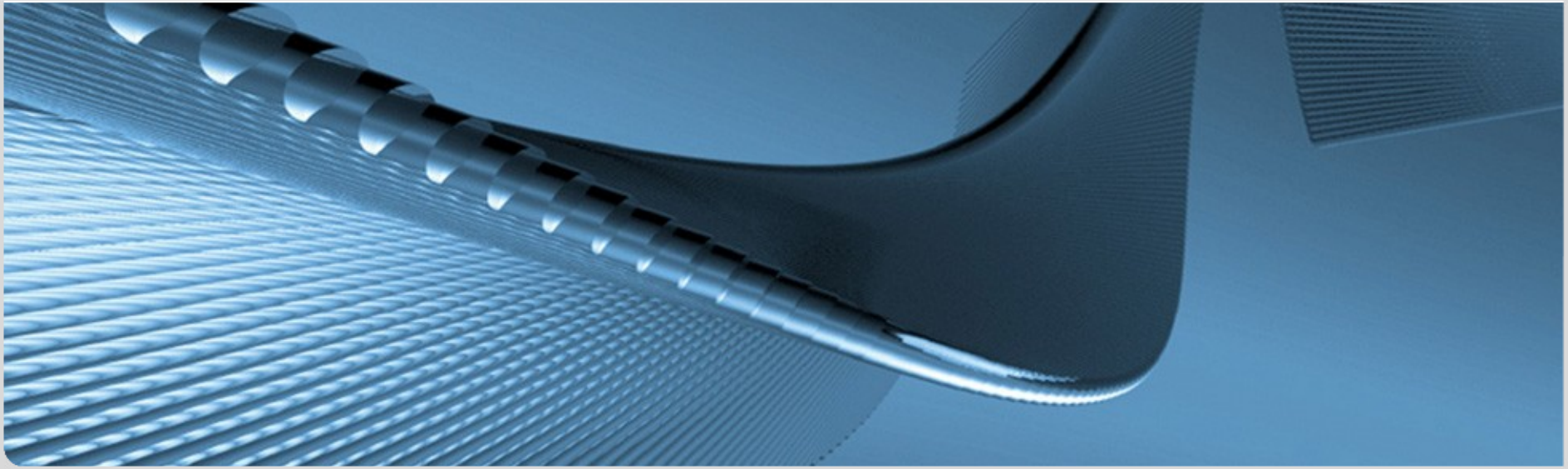
- Jeder Bürger soll selbst bestimmen, und
- Jeder Bürger soll wissen,
  - wer was wann und unter welchen Bedingungen
    - über ihn weiß.
    - über ihn in Erfahrung bringen darf.
- Ausnahmen nur auf gesetzlicher Basis
  - wenn das Interesse Dritter bzw. der Allgemeinheit schwerer wiegt als die Schutzinteressen des Betroffenen
- Bundesdatenschutzgesetz, §3, Abs. (1)

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person

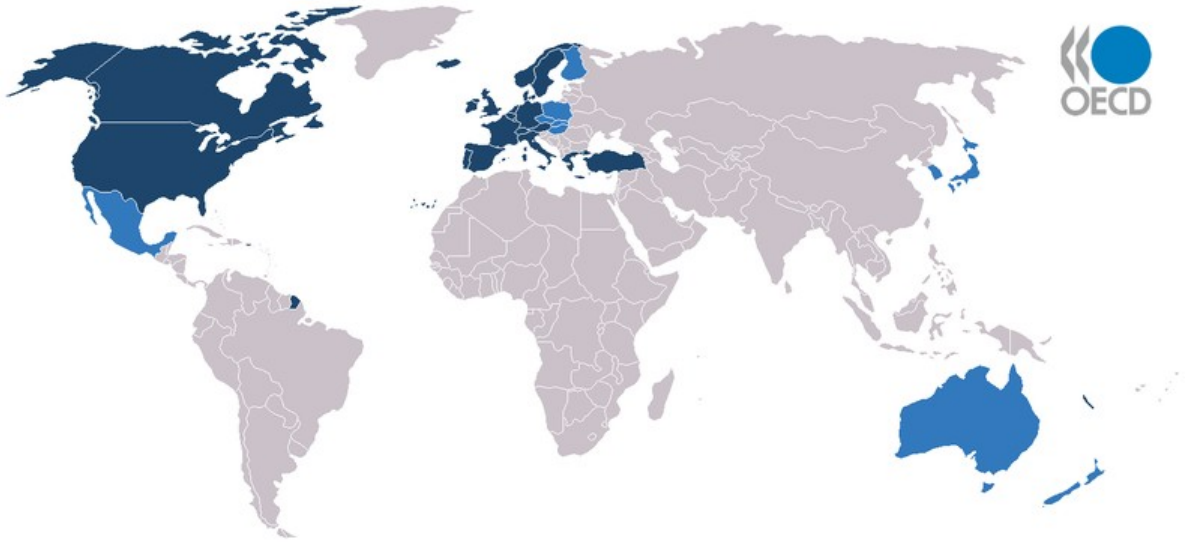
Karlsruher Institut für Technologie

Datenschutz International

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



Die OECD



- “Organisation für wirtschaftliche Zusammenarbeit und Entwicklung”
  - 34 Mitgliedsstaaten (meist entwickelte Länder)
  - Förderung von Wirtschaftswachstum, Welthandel, freier Waren- und Kapitalverkehr
    → hier gemeinsame Datenschutzstandards wichtig!
  - spricht (nicht rechtsverbindliche) Empfehlungen aus

Die OECD-Datenschutzempfehlungen (1/3)

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  - Empfehlung von 1980

    "The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. […] On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers..." [1]

    → es geht um gemeinsame Standards und den freien Datenaustausch

Die OECD-Datenschutzempfehlungen (2/3)

- **Collection Limitation Principle**
  - Daten nur sammeln falls erforderlich, und zwar so, dass der Betroffene es erfährt ("*by fair means*")
- **Data Quality Principle**
  - Daten sollen aktuell, korrekt und vollständig sein, damit der Betroffene nicht unter Fehlentscheidungen zu leiden hat
- **Purpose Specification Principle**
  - der Betroffene soll den Zweck der Datenerhebung spätestens zum Erhebungszeitpunkt erfahren
- **Use Limitation Principle**
  - Daten sollen nur für den spezifizierten Zweck verwendet und übermittelt werden

Die OECD-Datenschutzempfehlungen (3/3)

- **Security Safeguards Principle**
  - Schutz gegen Verlust, unautorisierten Zugriff etc.
- **Openness Principle**
  - Handhabung personenbezogener Daten soll für den Betroffnen transparent sein
- **Individual Participation Principle**
  - Betroffene sollen abfragen können, was über sie gespeichert wird, und was mit den Daten passiert
- **Accountability Principle**
  - Ansprechpartner für Beschwerden

"...These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties..." [1]

Umsetzung der OECD-Empfehlungen

- auf *freiwilliger* Basis (kein bindendes Völkerrecht!)
  - Asia-Pacific Economic Cooperation Privacy Framework
  - Federal Trade Commission, Report to the Congress, “Fair Information Practice Principles”, (USA)
  - Personal Information Protection and Electronic Documents Act (Kanada)
  - **EG-Richtlinien in Europa**

Europa und die OECD

- An der OECD (unter anderem) beteiligt:
  - die Länder der EU
  - die *Europäische Kommission* als unabhängiges, supranationales Organ der EU
    - von den Mitgliedsstaaten ernanntes Kolleg von Kommissaren
    - kann als einziges EU-Gremium formal EU-Rechtsvorschriften *vorschlagen*

→ **Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr**

Rechtsorgane in Europa (1/2)

- Europäische Gemeinschaft vs. Europäische Union
  - EU-Recht ist Völkerrecht,
    - regelt das Verhältnis zwischen den EU-Staaten
  - EG-Recht ist supranationales Recht
    - greift in die Rechte der Individuen ein
    - muss in den nationalen Rechtssystemen der EU-Mitgliedsstaaten umgesetzt werden

- *Anm.: Wenn ein Verkäufer auf eBay von EU-Recht schreibt, ist das Unsinn – außer er versteigert ein Land*

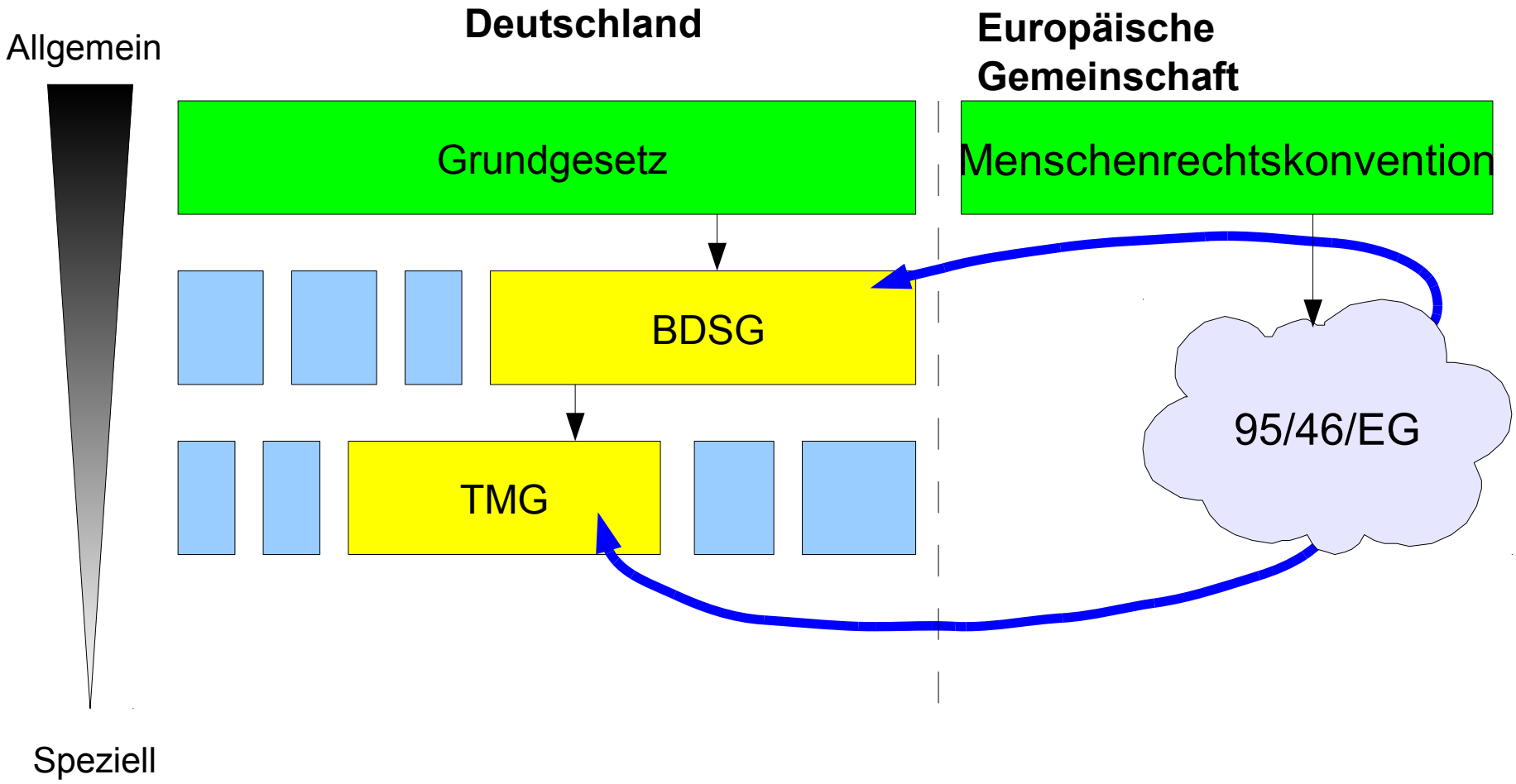
Rechtsorgane in Europa (2/2)

- Europarat
  - allgemeines Forum für Debatten über Zielsetzung der europäischen Politik
  - zwischenstaatliche Abkommen (KEINE Gesetze oder Richtlinien!)
    → *Europäische Menschenrechtskonvention*
- Europäische Kommission
  - Legislative, *Initiativrecht und Verabschiedung von Richtlinien*
  - Exekutive, *Überwachung der Umsetzung und Einhaltung der Richtlinien*
  - Kommissare werden von den EU-Staaten bestimmt
- Europa-Parlament
  - Wählt Präsident der EU-Kommission, *Annahme von Richtlinien*
  - Mitglieder alle 5 Jahre von den EU-Bürgern demokratisch gewählt
- Europa-Ministerrat
  - repräsentiert die Regierungen der EU-Staaten
  - verschiedene Zusammensetzungen, z.B. Rat für Justiz und Inneres → Treffen der Justizminister der Staaten
  - Nominiert Präsident der EU-Kommission, *Annahme von Richtlinien*

Wie EU-Richtlinien entstehen

1. EU-Kommission beauftragt zuständige Fachkommission
   - Fachkommission (z.B. „Inneres“ für Vorratsdatenspeicherung oder „Justiz“ für Datenschutz) arbeitet Vorschlag für Richtlinie aus
     - Konsultation mit Industrie und Parteien der Mitgliedsstaaten
2. Rücksprache mit den allen Kommissaren der EU-Kommission
   - Vorschlag wird einstimmig beschlossen
3. Europa-Parlament
   - wählt zuständigen Ausschuss (Beratungen, Expertenanhörungen)
   - Änderungsanträge
4. Europa-Ministerrat
   - interne Verhandlungen mit den Ministern der EU-Mitgliedsstaaten
   - Änderungsanträge
5. Lesung vor dem Europa-Parlament
   - Annahme oder
   - zurück an den Ausschuss, 2., 3. Lesung vor dem Parlament

Datenschutzrecht im europäischen Rahmen



Richtlinie 95/46/EG

- Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Anm.: engl. 95/46/EC)
  - vorgeschlagen von der Europäischen Kommission, verabschiedet vom Europäischen Parlament und Europa-Rat
  - musste von jedem EU-Mitgliedsstaat in Dreijahresfrist in nationales Recht überführt werden
    - in Deutschland erst 2001 nach Vertragsverletzungsverfahren
  - harmonisiert Datenschutzrecht innerhalb von Europa
    → äquivalente Standards, obwohl Detailfragen von Land zu Land unterschiedlich geregelt

Abgrenzung zu anderen DS-Richtlinien

- 95/46/EG ist eine übergeordnete Richtlinie zum Datenschutz, die durch spezialisierte Datenschutz-Richtlinien ergänzt wird
  - Richtlinie 2002/58/EG
    - Datenschutzrichtlinie für elektronische Kommunikation
    - beschränkt auf Telekommunikationsdienste, d.h., Vertraulichkeit der Kommunikation, Abrechnungsdaten
  - Richtlinie 2006/24/EG
    - Vorratsdatenspeicherung
    - Daten für einen bestimmten Zeitraum zum Zweck der Ermittlung und Verfolgung von schweren Straftaten aufbewahrt werden.

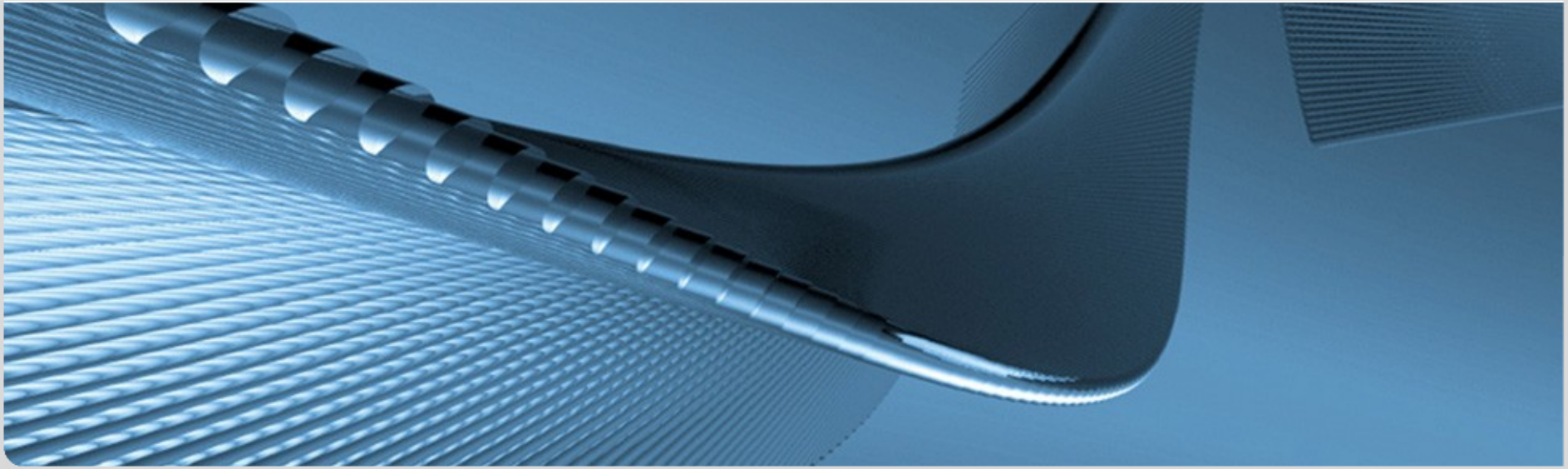
Inhalt von 95/46/EG

- Erwägungsgründe für die Richtlinie
  - wichtig für teleologische und systematische Auslegung
- Geltungsbereich
  - weit gefasst: *“...alle personenbezogenen Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen...”*
  - erstreckt sich explizit nicht auf strafrechtliche Bereiche sowie persönliche/familiäre Tätigkeiten
- Umsetzung der OECD-Empfehlungen

Karlsruher Institut für Technologie

Datenschutz Deutschland

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



Welches Recht ist anzuwenden?

- Deutsches Recht?
  - Niederlassung oder Standort des Verantwortlichen in Deutschland (Herkunftslandprinzip, §3 Abs.2 TMG)
- Rechtsnorm
  - das spezifische Gesetz verdrängt das allgemeine Gesetz
  - und andersherum: wenn kein spezifisches Gesetz vorhanden, gilt das allgemeine (bis hinauf zum Grundgesetz)

Wie funktioniert deutsches Recht?

- Offensichtlich kann es keine Einzelnorm für jeden Fall geben
  - Prognostische Fähigkeiten des Gesetzgebers sind begrenzt
  - Aufwand bei der Regulierung zu hoch, Aktualisierung zu aufwendig, Kontrolle und Durchsetzung zu schwierig
- Lösung:
  - Hierarchie von Normen
    - oberste Ebene: Grundgesetz; verfeinert durch weitere Gesetze und Normen
    - wenn keine passendere Spezialnorm existiert, ist die allgemeine anzuwenden
  - Auslegungskanon
    - Interpretation des Wortlautes, um möglichst nahe an der **Intention** des Gesetzgebers zu bleiben

Auslegung von Normen (1/3)

- **Grammatische Auslegung**
  - *nach dem Wortlaut;* Fall im Gesetz berücksichtigt
  - Problem: Gesetzgeber hat nur beschränkte prognostische Kraft, kann keine zukünftigen Fälle vorhersehen; Normziel aber oft langfristig beständig

- **Teleologische Auslegung**
  - *nach dem Sinn und Zweck* (Telos: griech. Ziel);
    Was hat der Gesetzgeber mit der Norm intendiert?
    - Wenn der Gesetzgeber die Datenerhebung mit einer bestimmten Technologie reguliert, hat er ebenfalls Datenerhebungen mit vergleichbaren Technologien geregelt, selbst wenn diese nicht genannt werden.
  - Problem: oft viel Spielraum bei der Interpretation

Auslegung von Normen (2/3)

- **Historische Auslegung**
  - *dogmengeschichtlich*: in welche Richtung entwickelt sich die Gesetzgebung?
    - Sinnfestsetzung über Vorläufernormen oder existierende Urteile der Gerichte
  - *genetische Auslegung:* Sinnfestsetzung über andere Texte
    - Parlamentsberatungen, amtliche Begründungen
  - Problem: kein einheitlicher, kontinuierlicher Gesetzeswille; Ziele der Gesetzgebung können sich zeitlich wandeln

Auslegung von Normen (3/3)

- **Systematische Auslegung**
  - *nach dem Gesamtkontext:* Bestimmung durch Rückschlüsse aus der Stellung der Norm im Gefüge des Gesetzes bzw. anderer Normen
    - Beispiel: *Ausnahmeregelungen sind grundsätzlich eng auszulegen* (sonst wären es ja keine Ausnahmen im Kontext der Norm, sondern Standardfälle)
  - Problem: Rechtsordnung müsste als ganzes konsistent und widerspruchsfrei sein, damit das funktioniert

- Nach allg. Verständnis kein Rangverhältnis zwischen den Auslegungsarten, sinnvoll ist jedoch oft die Anwendung in der hier gegebenen Reihenfolge

Anm.: in anderen Ländern funktioniert das z.T. anders!

Das Grundgesetz

- Art.1(1) GG: *Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.*

- Art. 2(1) GG: *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.*

→ Art. 2(1) GG in Verbindung mit Art.1(1) GG: Recht auf Informationelle Selbstbestimmung

Quelle: www.bundestag.de

Recht auf Informationelle Selbstbestimmung

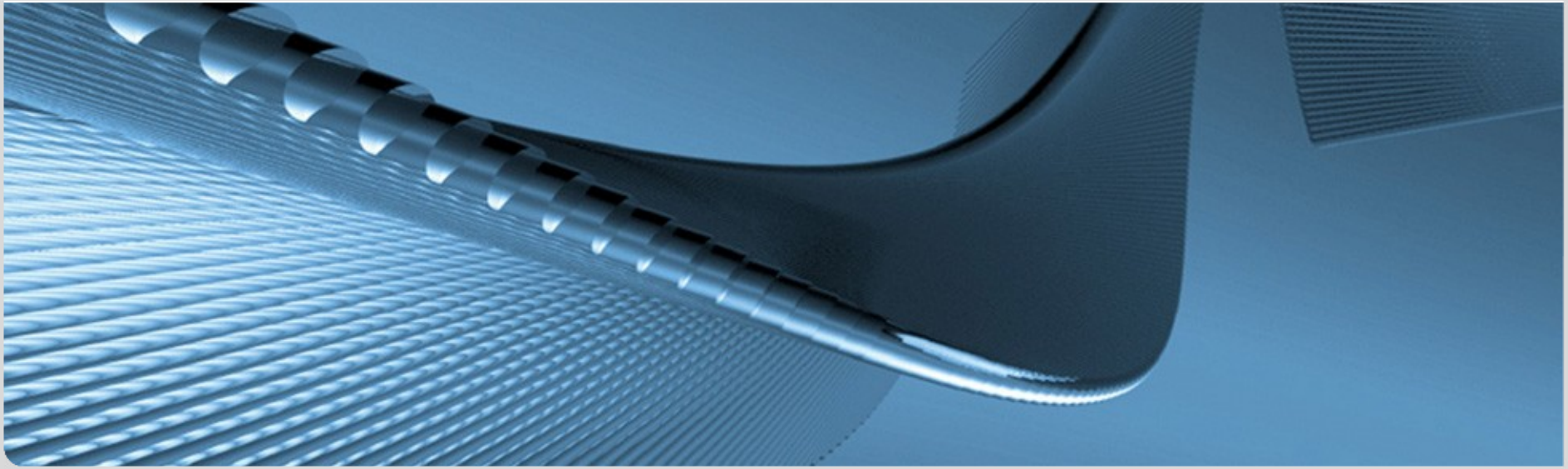
- Volkszählungsurteil BVerfGE 65, 1 von 1983:
  “Jeder kann selbst über die Weitergabe und Verwendung persönlicher Daten entscheiden, er kann bestimmen, in welchen Grenzen Lebensumstände zu offenbaren sind."

- Datenschutz als Grundrecht
  - **Einschränkung nur auf gesetzlicher Grundlage**
    (GG: ...*soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt)*
    - Beispiel: Ein Dieb im Kaufhaus kann keine Datenschutzrechte gegen Überwachungskameras geltend machen.

Karlsruher Institut für Technologie

Das Bundesdatenschutzgesetz

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



Das Bundesdatenschutzgesetz (BDSG)

- Abschnitte des BDSG

1.	Allgemeine Bestimmungen	• Begriffsbestimmung, • Grundregeln, • Anwendungsgebiete
2.	Datenverarbeitung der öffentlichen Stellen	• Rechtsgrundlagen • Rechte des Betroffenen • Bundesbeauftragter für den Datenschutz
3.	Datenverarbeitung nichtöffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen	• Rechtsgrundlagen • Rechte des Betroffenen • Aufsichtsbehörde
4. 5. 6.	Sonder- Schluss- und Übergangsvorschriften	• Forschung, Medien, Amtsgeheimnisse • Bußgeld- und Strafvorschriften

Begriffsbestimmung (1/3)

- **Verantwortliche Stelle** ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
- **Empfänger** ist jede Person oder Stelle, die Daten erhält.
- **Dritter** ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.
- **Öffentliche Stellen des Bundes** sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes
- **Öffentliche Stellen der Länder** sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde etc.

Begriffsbestimmung (2/3)

- **Automatisierte Verarbeitung** ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.
- **Erheben** ist das Beschaffen von Daten über den Betroffenen.
- **Verarbeiten** ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.
- **Nutzen** ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Begriffsbestimmung (3/3)

- **Besondere Arten** personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
- **Anonymisieren** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
- **Pseudonymisieren** ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen.

Prinzipien des BDSG

- Informationelle Selbstbestimmung als **Abwehrrecht** gegenüber hoheitlichem Handeln
- Daten kann man
  - erheben
  - verwenden
    - verarbeiten
      - speichern
      - verändern
      - übermitteln
      - löschen, sperren
    - nutzen

  → *es existieren Normen für jeden dieser Fälle*

Verarbeiten vs. Nutzen, Löschen vs. Sperren

- Verarbeiten:
  - inhaltliches umgestalten, verändern der Daten
  - in Zusammenhangsetzen, Zusammenhang entfernen
  - auch Korrektur, Löschung

  → es entsteht eine neue Aussage
- Nutzen:
  - alles andere

- Löschen:
  - entfernen der Daten
- Sperren:
  - Daten werden unzugänglich, sind aber noch vorhanden (z.B. für gesetzliche Nachweispflichten)

Erhebung (1/3)

- §3a BDSG: **Datenvermeidung** und **Datensparsamkeit**
  - keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen
  - Anonymisierung und Pseudonymisierung soweit möglich, und Aufwand in einem angemessenen Verhältnis zum Schutzzweck

- §4 BDSG: Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
  - Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit gesetzlich erlaubt oder der Betroffene einwilligt
    → **Verbot mit Erlaubnisvorbehalt**
  - **Pflicht zur Direkterhebung**, es sei denn es existiert eine anderslautende Rechtsvorschrift

Erhebung (2/3)

- §4 BDSG:
  - **Auskunftspflicht**; der Betroffene ist von der verantwortlichen Stelle über
    - Identität der verantwortlichen Stelle,
    - Zweckbestimmungen der Erhebung, Verarbeitung, Nutzung
    - die Kategorien von Empfängern der Daten
  - Auskunftspflicht gilt nur, sofern der Betroffene nicht bereits anderweitig von diesen Informationen Kenntnis erhalten hat

Erhebung (3/3)

- Erforderlichkeitsprinzip
  - §13 BDSG: öffentliche Stellen
    - zulässig, wenn Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich
  - §28 BDSG: nichtöffentliche Stellen
    - zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses dient,
    - soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist, oder
    - wenn die Daten allgemein zugänglich sind
    - es sei denn: “...Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen ...überwiegt.”
- Alle anderen Arten der Datenerhebung sind verboten!

Einwilligung

- §4a BDSG: **Einwilligung** ist nur wirksam, wenn
  - freien Entscheidung des Betroffenen
  - Information über Zweck und Folgen der Verweigerung der Einwilligung
  - Einwilligung in Schriftform, soweit nicht andere Form angemessener ist
  - Ausnahmen für wissenschaftliche Forschung

Übermittlung

- §4b BDSG: **Übermittlung** personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen
  - Unterscheidung nach
    - EU-Mitgliedern (siehe Richtlinie 95/46/EG)
    - Ländern ohne “angemessenes Datenschutzniveau”
      - USA, abgesehen von Unternehmen des Safe-Harbor-Abkommens
  - weitreichende Auskunftspflichten

Betroffenenrechte

- §6 BDSG: Unabdingbare Rechte des Betroffenen
  - Rechte auf **Auskunft** (§19, §34 BDSG), **Berichtigung**, **Löschung** oder **Sperrung** (§20, §35 BDSG) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.
  - Bei mehreren verantwortlichen Stellen können diese Rechte bei jeder Stelle beansprucht werden
    → Anspruch muss passend weitergeleitet werden

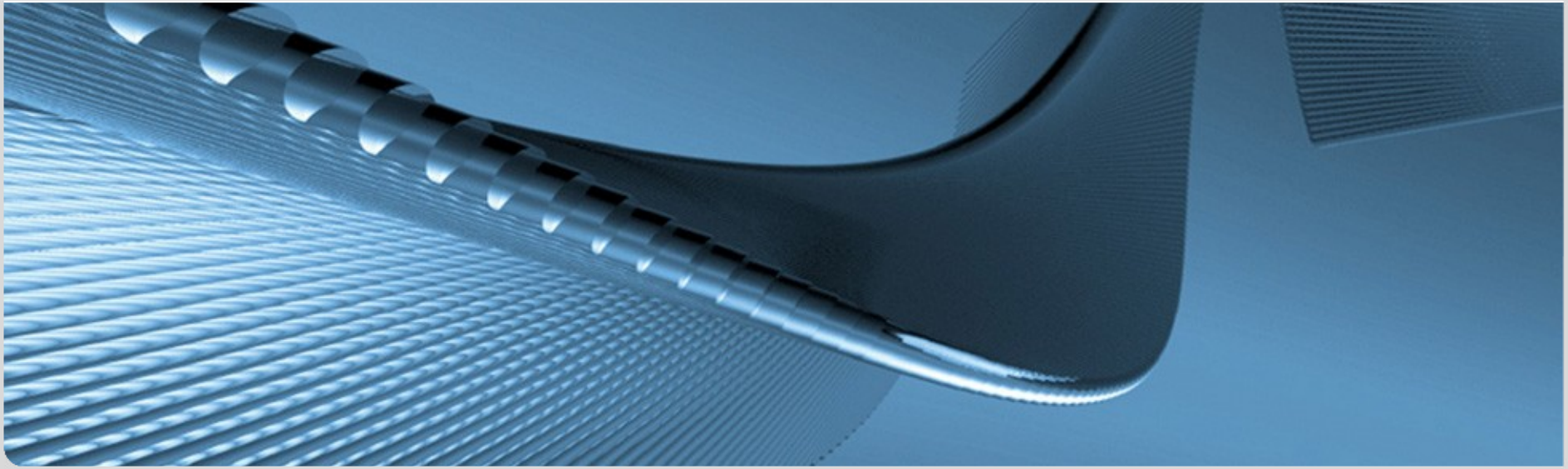
BDSG zielt auf Systemdatenschutz ab!

- Ganzheitliche organisatorische und technische Maßnahmen zum Datenschutz
  - Prinzip der Datenvermeidung
    - Entwicklung von Datenverarbeitungsprozessen, die mit wenig Daten auskommen
    - Daten, die nicht erhoben wurden, können auch nicht verloren gehen oder mißbraucht werden
  - Vorrang anonymer und pseudonymer Datenverarbeitung
    - möglichst kleine digitale Teilidentität
    - Verkettbarkeit einschränken

Karlsruher Institut für Technologie

Das Telemediengesetz

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



Das Telemediengesetz (TMG)

- zentrales Gesetz zur Regulierung des Internets
  - nicht nur Datenschutzfragen
- Umsetzung von Richtlinie 2000/31/EG (e-Commerce)
  + Datenschutznormen
- Geltungsbereich:
  - alle Anbieter elektronischer Informations- und Kommunikationsdienste
  - *Nicht*: reine Telekommunikationsdienste, also Zugangsprovider, Backbonebetreiber oder Mobilfunkanbieter

- *im folgenden: einige der interessantesten Paragraphen*

Allgemeine Informationspflicht

- §5 Abs. 1 TMG: bei geschäftsmäßiger Tätigkeit müssen Name, Anschrift, Rechtsform, zuständige Aufsichtsbehörde, Handelsregistereinträge etc.
  - *leicht erkennbar*
  - *unmittelbar erreichbar* und
  - *ständig verfügbar* sein.
- Angabe eines Impressums auf der Webseite jedes *geschäftsmäßigen* Anbieters
  - *geschäftsmäßig* bedeutet nicht unbedingt mit kommerziell; auch ein Privatmann kann geschäftsmäßig handeln!
  - Maßstab: Umfang der Tätigkeiten

Verantwortlichkeiten

- §8, §9, §10 TMG: *Durchleiten, Zwischenspeichern* (Caches von Web-Proxies) und *Speichern* von Informationen macht den Betreiber nicht automatisch zur verantwortlichen Stelle
  - sofern er die Übermittlung nicht veranlasst,
  - die Adressaten nicht ausgesucht,
  - die Informationen nicht verarbeitet und
  - keine Kenntnis von rechtswidrigen Inhalten hat.
    (Anm.: stark verkürzte Darstellung; das TMG ist hier deutlich präziser)

→ Keine Verantwortung für fremde Informationen, jedenfalls unter Beachtung einiger Einschränkungen

Pflichten des Dienstanbieters

- §13 Abs.1 TMG: *zu Beginn der Nutzung* Unterrichtung über
  - Zweck und Umfang der Erhebung personenbezogener Daten
  - Datenverarbeitung außerhalb des Geltungsbereichs von Richtlinie 95/46/EG
    - nicht EU und keine ähnlichen Datenschutzstandards
  - *“...automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet...”*
    - Cookies, Web-Bugs

Elektronische Einwilligung

- Erforderlich nach §12 Abs.1, 2 TMG, wenn pers. Daten für Zwecke genutzt werden, die nicht ausdrücklich in einem Gesetz für Telemedien erlaubt sind
- §13 Abs. 2 TMG: Elektronische Einwilligung, wenn sie
  - bewusst und eindeutig erfolgt,
  - protokolliert wird und vom Nutzer jederzeit abrufbar ist
  - der Nutzer jederzeit widerrufen kann
    → Hinweis darauf erforderlich (§13 Abs. 3 TMG)

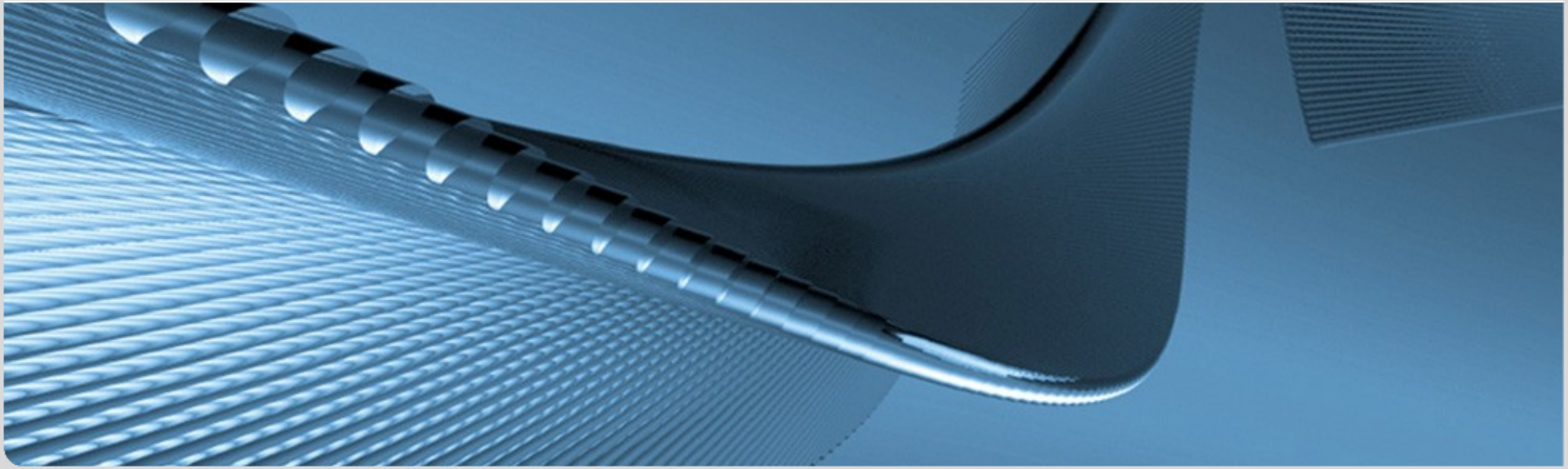
Weitere Rechte des Nutzers (Auszug)

- Diensterbringer muss sicherstellen (§13 Abs. 4 TMG)
  - Nutzung kann jederzeit beendet werden
  - anfallende pers. Daten werden nach Nutzungsende gelöscht oder gesperrt
  - Nutzungsdaten nur für Abrechnungszwecke
  - Nutzungsprofile nicht mit Angaben zur Identifikation des betroffenen verknüpfen
- Betreiber muss Nutzung und Zahlung von Telemedien anonym bzw. prseudonym ermöglichen, sofern technisch möglich und zumutbar (§13 Abs. 6 TMG)
  → *leider nicht klar was "zumutbar" bedeutet*
- jederzeit mögliches Auskunftsersuchen: §13 Abs. 7 TMG
- Datenschutzverstöße werden klar als Ordungswidrigkeiten definiert (§16 TMG)

Karlsruher Institut für Technologie

Vorratsdatenspeicherung

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“



Vorratsdatenspeicherung (VDS)

- Telekommunikationsdienstleister speichern **Verkehrsdaten**
  - Telefon: Nummern, Zeiten
  - Handy, SMS: zusätzlich noch die Funkzellen
  - Email, Chat: IP-Adressen, Absender und Empfänger, Server
  - …
- Nur **öffentlich zugängliche** Dienstleister
  - keine Mails im Firmennetzwerk
- Nur **Telekommunikation**
  - Webseiten-Abrufe dürfen nicht Personen zugeordnet werden (es sei denn Web-Chat, Web-Mail)
- **befristete** Speicherdauer
  - Richtlinie 2006/24/EG: min. 6 Monate, max. 2 Jahre

Geschichte

- 2004, Zuganschläge von Madrid: Europäischer Rat beauftragt Prüfung einer Richtlinie zur VDS
- 2005, Anschläge in London: EU-Kommission schlägt Richtlinie vor
- 2006: Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die VDS
- Dez. 2007, Deutschland: Umsetzung durch das Gesetz zur Neuregelung der TK-Überwachung
  - Änderungen in Telekommunikationsgesetz, Strafprozeßordnung
- Mär. 2010: Gesetz gekippt vom Bundesverfassungsgericht
  - aktuell keine VDS in Deutschland
- Apr. 2011: Evaluation der Richtlinie 2006/24/EG
- Jun. 2011. EU-Kommission fordert Stellungnahme des BJM an
  - erste Stufe eines Vertragsverletzungsverfahrens wegen der nicht erfolgten Umsetzung der EU-Richtlinie

Pro und Kontra

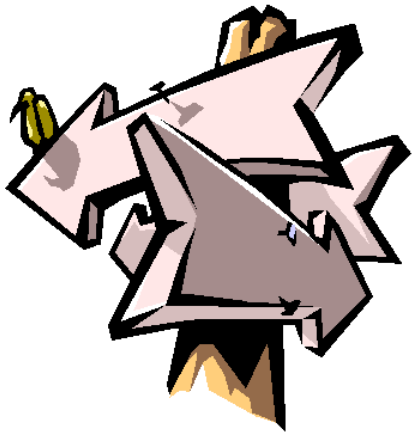
- Argumente für VDS
  - Terrorismusabwehr
  - Aufklärung schwerer Straftaten
- Argumente dagegen
  - Verhältnismäßigkeit
  - Effektivität
    - einfache Umgehung der VDS (→ nächste Folie)
    - Aufklärungsquote bei der Strafverfolgung durch VDS nicht höher
    - VDS verhindert keine Terroranschläge, da nur forensische Auswertung
  - vorhandene Alternativen (→ nächste Folie)
  - teure Umsetzung
    - beispiel Telekom: 19 TB Verkehrsdaten für 6 Monate VDS

Wirksamkeit

- VDS ist **sehr** leicht zu umgehen
  - Prepaid-Mobiltelefone, öffentliche Telefonzellen, Voice-over-IP
  - offene WLAN-Hotspots
  - nichtöffentliche Firmen-Mailserver
  - Anonymisierungsdienste mit Servern außerhalb der EU
    - Privoxy, JAP, Tor

Bild: AK Vorrats-datenspeicherung

Alternativen



- darauf verzichten
  - zu Abrechnungszwecken werden Verkehrsdaten ohnehin aufbewahrt
  - Zugriff darauf nach Gerichtsanordnung möglich
  - hohe Aufklärungsquote der Polizei rechtfertigt keine VDS
- Quick Freeze (aktueller Vorschlag unserer Justizministerin)
  - bei Anfangsverdacht Verkehrsdaten Verdächtiger länger speichern
    - Normalfall: Unternehmen löschen unnötige Verkehrsdaten nach einigen Tagen
  - Freigabe dieser Daten für Ermittlung erst nach Gerichtsanordnung

Bundesverfassungsgericht im März 2010

- Ausgestaltung der Vorratsdatenspeicherung nicht Verfassungskonform
  - *„ Zwar ist eine Speicherungspflicht [...] nicht [...] verfassungswidrig. Es fehlt aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisten weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Auch genügen sie nicht […] Transparenz und Rechtsschutzanforderungen.“*

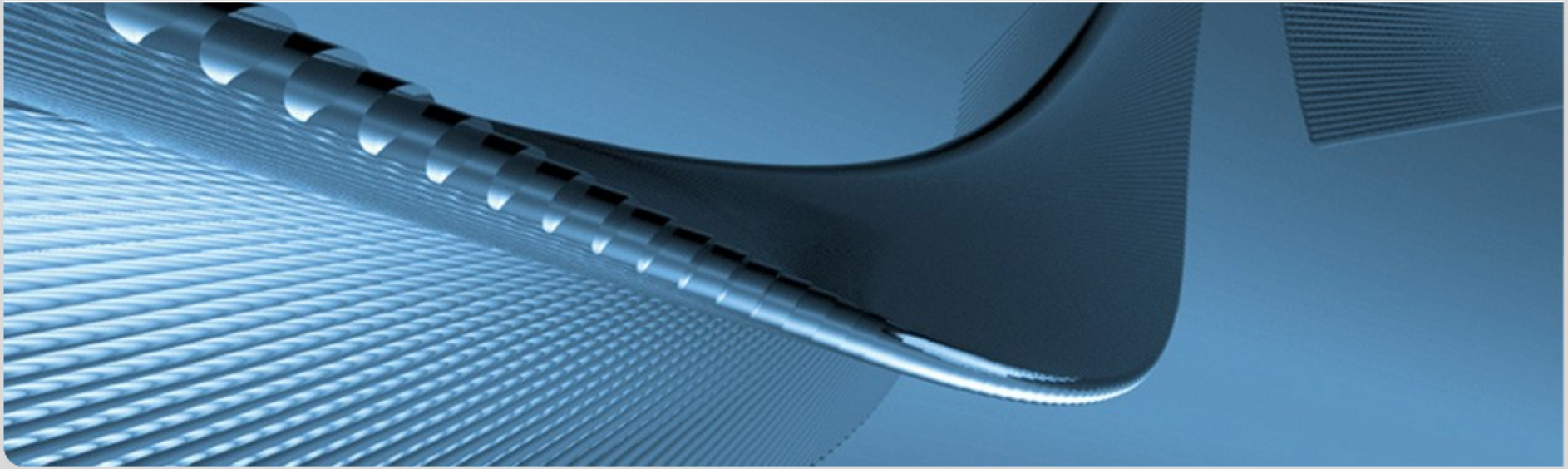
- konkrete Kritik in 5 Punkten:
  - anlasslose Speicherung muss Ausnahme bleiben
  - Vorkehrungen für Datenschutz und -sicherheit unzureichend
  - Kriterien für die Datennutzung zu weit gefasst
  - Vorratsdatenspeicherung muss für Betroffene transparent sein, Strafverfolgung ≠ Geheimdienst
  - nachträgliche gerichtliche Kontrolle

EU-Kommission im April 2011

- Evaluationsbericht zur Vorratsdatenspeicherung in Europa
  - Fallbeispiele zur Nützlichkeit der VDS
    - Kinderpornographie, Drogenschmuggel, Telefonbetrüger
- VDS-Daten unterschiedlich genutzt (Zahlen 2008)
  - entweder extrem selten (Zypern 34, Griechenland 584, Dänemark 3.600) oder extrem oft (Tschechien 131.500, England 470.000)
    → unklare Kriterien
  - Deutschland: 12.600 Abrufe
  - die meisten Abrufe betrafen Daten jünger als 3 Monate
    → Quick Freeze wäre möglich
- EU-Innenkommissarin Malmström hat nur Positiv-Fälle gesammelt
  - sehr (!) wenige Fallbeispiele
  - wären diese Fälle auch ohne VDS gelöst worden?
- *Richtlinie soll überarbeitet werden*

Karlsruher Institut für Technologie

Abschluss



Fazit BDSG, TMG

- TMG, BDSG entsprechen den OECD-Empfehlungen
- TMG hat Überschneidungen mit BDSG;
  manche Pflichten werden hier nochmals aufgeführt,
  z.B. Auskunftsanspruch, Recht auf Löschung
  → betont Wichtigkeit
- etliche Normen betreffen unternehmensinterne Vorgäng
  → Kontrolle und Durchsetzung praktisch unmöglich
- etliche Normen werden durch weiche Begriffe eher zu Empfehlungen
  - "...soweit technisch möglich und zumutbar..."

Zusammenfassung der Vorlesung

- Grobe Orientierung im Datenschutzrecht
  - Einordnung des deutschen DS-Rechts in den internationalen Rahmen
  - Leitfaden zur Interpretation der Rechtsvorschriften
  - Aufbau und Inhalt des BDSG, wesentliche Normen des TMG; Schwerpunkt auf Regelungen fürs Internet
- Was wurde ausgelassen?
  - zahlreiche Details
  - Rechtsnormen für andere Bereiche, z.B. Telekommunikationsanbieter
  - Länderspezifische Regelungen;
    jedes Bundesland hat ein Landesdatenschutzgesetz

Literatur

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org

[2] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, http://ec.europa.eu

[3] BDSG, http://bundesrecht.juris.de/bdsg_1990/index.html

[4] TMG, http://www.gesetze-im-internet.de/tmg