

IT-Sicherheitstagung Diakonie
26. Januar 2009

Datenschutz und IT-Sicherheit

Dr. jur. Alexander Koch
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Datenschutzrecht

- **Verfassung:**
 - Recht auf informationelle Selbstbestimmung (1983 im Volkszählungsurteil des BVerfG in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verortet).
- **Allgemeines Datenschutzrecht:**
 - BDSG (sowie für den öffentlichen Bereich: DSG der Länder).
- **Sektorspezifisches Datenschutzrecht:**
 - TKG, TMG.

Grundsätze des Datenschutzes

- Jede Verarbeitung personenbezogener Daten bedarf einer gesetzlichen Ermächtigung.
- Die Daten müssen erforderlich sein.
- Die Daten dürfen nur solange aufbewahrt werden, wie sie benötigt werden.
- Daten müssen technisch und organisatorisch gegen Missbrauch gesichert sein (Anlage zu § 9 S. 1 BDSG!).

Fernmeldegeheimnis

- **Verfassung:**
 - Art. 10 GG.
- **Einfachgesetzlich:**
 - § 88 TKG.
- **Unterschiede zum Datenschutzrecht:**
 - DatenschutzR: Bezug Person zu einem Datum.
 - Fernmeldegeheimnis: Inhalt der Fernkommunikation.

IT-Sicherheit ./. Datenschutz

- Problem: Firewalls, IDS, Virens Scanner, Spam- und WWW-Filter sind auf möglichst viele Daten angewiesen.
- Das Datenschutzrecht scheint dem häufig entgegenzustehen.
- Versöhnung zwischen IT-Sicherheit und Datenschutz ist aber möglich!

- Verhältnis zum BDSG.
- Verhältnis zum TMG.
- Anwendungsbereich: Diensteanbieter.
- Schutz des Fernmeldegeheimnisses: § 88 TKG / § 206 StGB (Mitteilen u. Unterdr.).
- Ermächtigung für Eingriffe:
 - § 109 TKG?
 - Technische Schutzmaßnahmen.
 - Norm zielt auf Schutz, gerade keine Ermächtigung. (-)

- Ermächtigung für Eingriffe:
 - § 100 Abs. 2 TKG? (-)
 - Zugriff auf Kommunikationsinhalte.
 - Nicht auf IP-Kommunikation übertragbar.
 - § 100 Abs. 3 TKG?
 - Bekämpfung rechtswidriger Inanspruchnahme.
 - Wohl keine allgemeine Ermächtigung. (-)
 - § 100 Abs. 1 TKG?
 - Schutz von TK-Anlagen. (+)

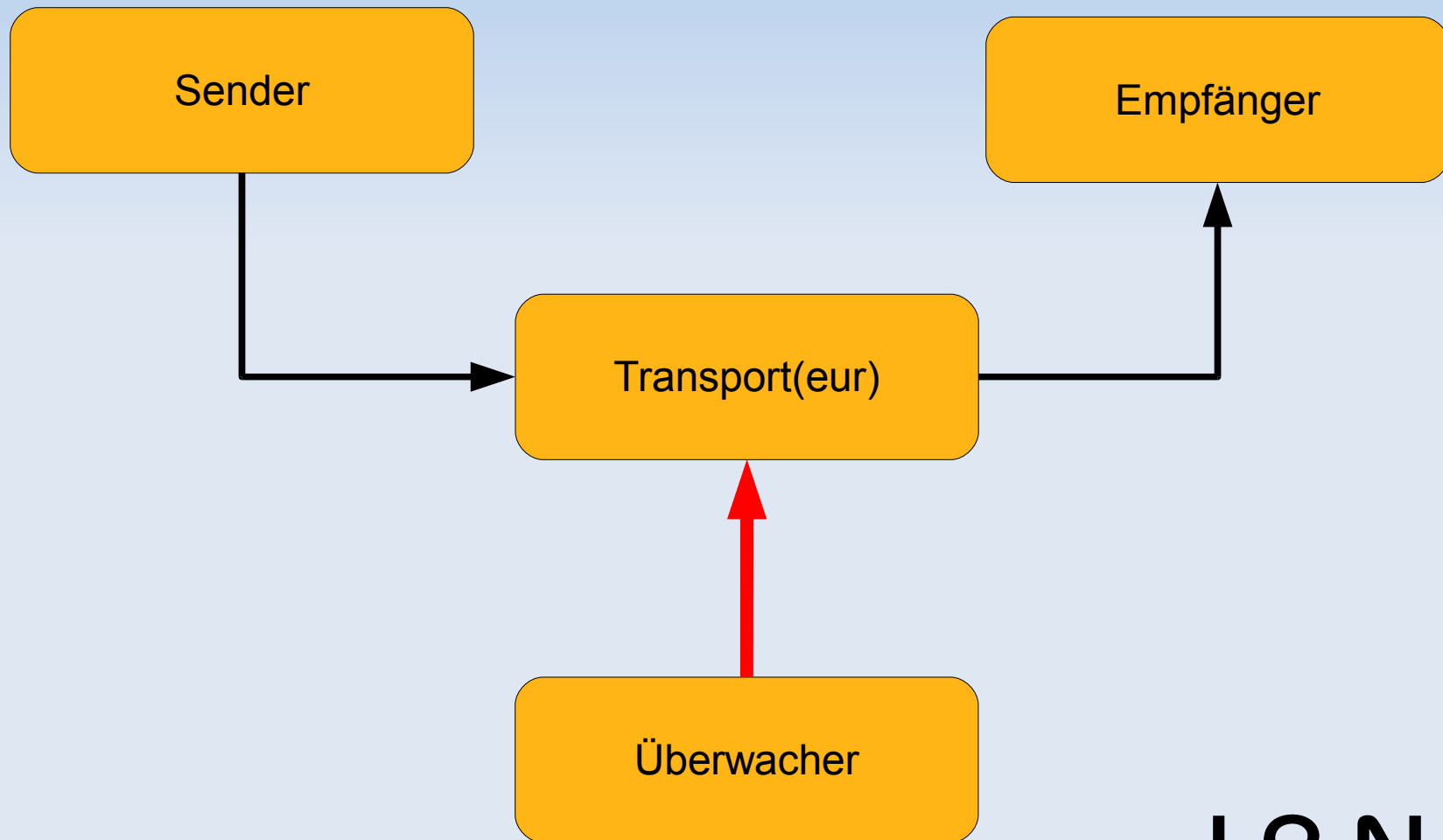
§ 100 Abs. 1 TKG

- Erkennen, Eingrenzen oder Beseitigen
- von Störungen oder Fehlern
- an TK-Anlagen,
 - also keine Endgeräte!
- Bestands- und Verkehrsdaten.
 - Keine Inhaltsdaten!
- D.h.:
 - Viren- und Spamfilter (?),
 - Firewalls (+),
 - IDS (-).

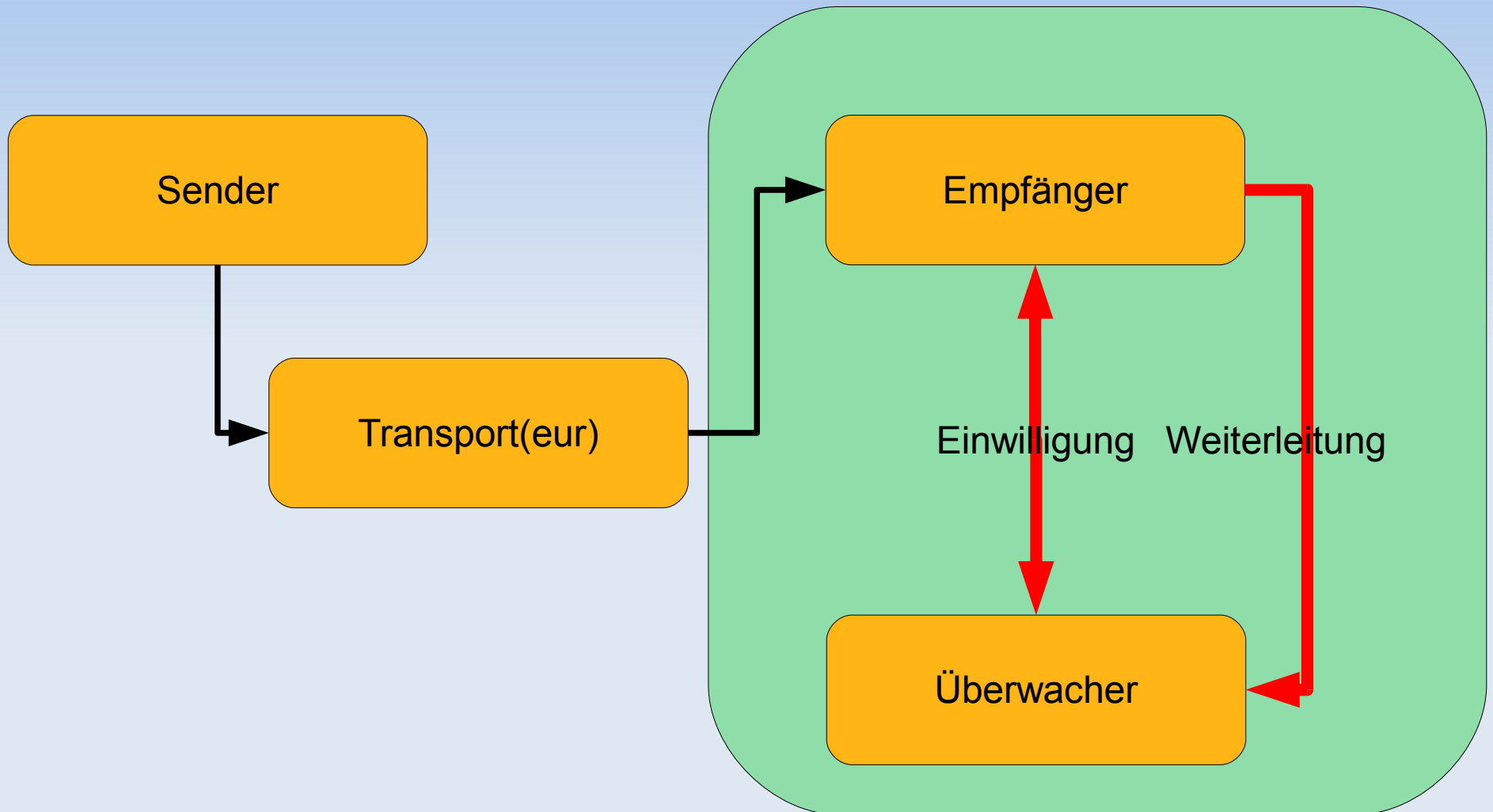
Lösung: Einwilligung!

- Problem: Es ist praktisch nur die Einwilligung der eigenen Angestellten, nicht aber von deren Kommunikationspartnern einholbar.
- Frage: Müssen beide Kommunikationspartner einwilligen?

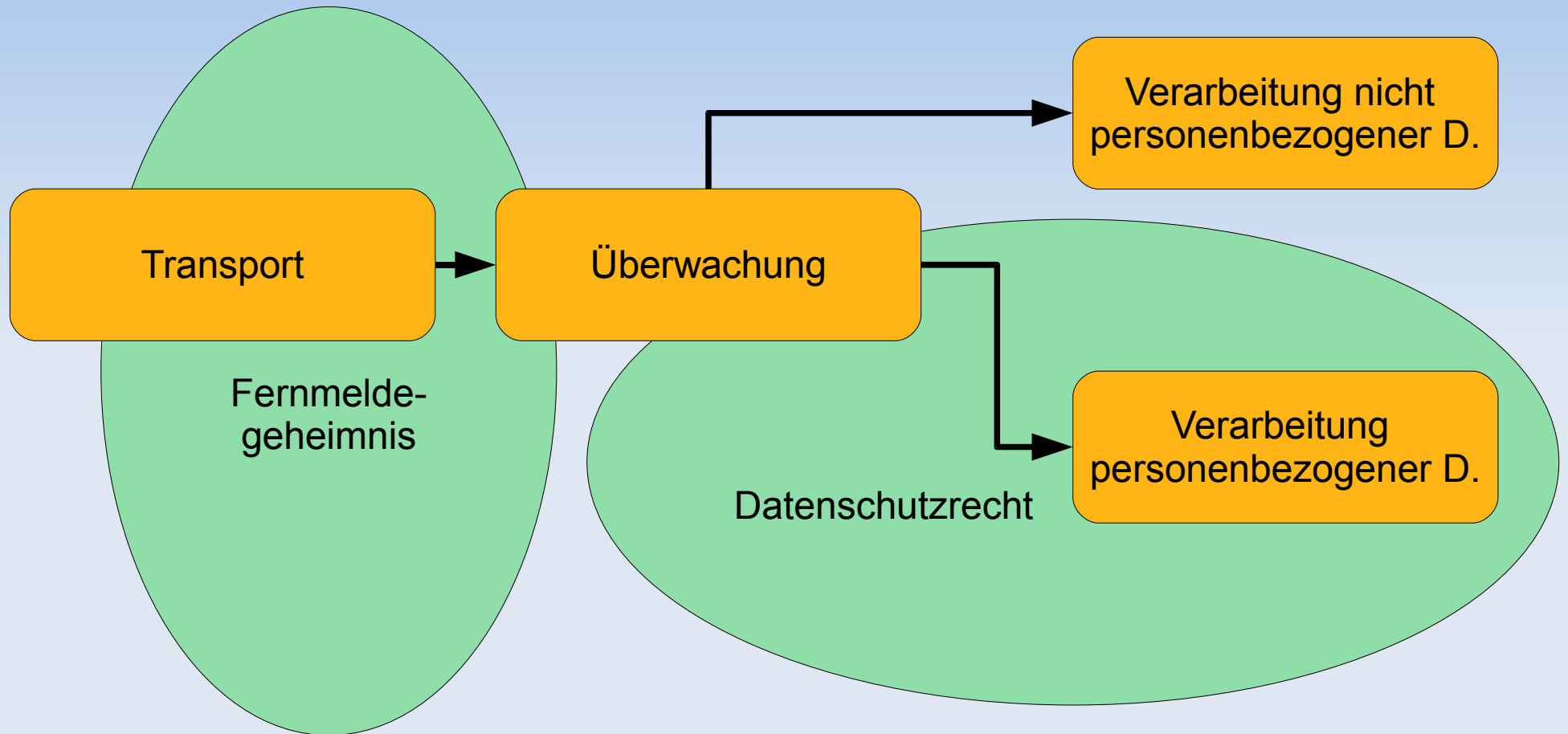
Struktur des FernmeldeG



Einwilligung und FernmeldeG



Datenschutz hinter dem FMG



§ 28 Abs. 1 Nr. 2 BDSG

- Wahrung berechtigter Interessen,
- erforderlich,
- keine schutzwürdigen Interessen des Betroffenen.

Telemediendatenschutz

- Problem insbesondere: Protokolldateien.
- Praktisch alle Server protokollieren in der Standardeinstellung IP-Adressen.

TM-Datenschutz

- § 12 TMG
 - Personenbezogene Daten dürfen nur erhoben und verwendet werden, soweit das TMG oder eine andere TM-Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.
- § 15 TMG
 - Personenbezogene Daten dürfen nur erhoben und verwendet werden, um die Inanspruchnahme zu ermöglichen und abzurechnen.

TM-Datenschutz

- § 15 Abs. 8 TMG
 - Bei „zu dokumentierende[n] tatsächliche[n] Anhaltspunkte[n]“ einer unentgeltlichen Nutzung dürfen personenbezogene Daten über das Ende des Nutzungsvorgangs gespeichert werden.
- Eine hierüber hinausgehende Regelung wie § 100 TKG fehlt im TMG!
 - TMG sieht also keine Datenverarbeitung aus Gründen der Systemsicherheit vor.
 - Wurde bereits zu Zeiten des TDG kritisiert.

AG Berlin, Urt. v. 23.11.2006

- Beklagte: Bundesrepublik Deutschland, vertreten durch das Bundesministerium der Justiz.
- Hintergrund: Das BMJ hat im WWW-Log IP-Adressen protokolliert.

Das Urteil im Einzelnen

- IP-Adressen haben Personenbezug.
 - Gilt auch für dynamische IP-Adressen.
 - Bei IP-Adressen ist der Betroffene jedenfalls bestimmbar.
 - Erwägungsgrund 26 der EG-Datenschutzrichtlinie: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.“

Das Urteil im Einzelnen

- Hilfsüberlegung: Ohne Personenbezug könnten Daten etwa an Zugangsanbieter weitergegeben werden, die die Zuordnung Nutzer-IP ohne Probleme herstellen könnten.
- Datenschutzrecht soll gerade auch vor Missbrauchskonstellationen schützen.

AG München, Urt. v. 30.9.2008

- Das Gericht stellt in einem obiter dictum fest, dass IP-Adressen *keine* personenbezogenen Daten sind.
- Obergerichtliche Klärung steht nach wie vor aus.

Umgang mit IP-Adressen

- IP-Adressen sollten nur um die beiden letzten Oktetts gekürzt gespeichert werden (192.168.xxx.yyy).
- Dem Vernehmen nach soll bei der nächsten TMG-Novelle eine dem § 100 TKG entsprechende Norm eingeführt werden.

Vielen Dank für die Aufmerksamkeit!

Für weitere Informationen:

IRNIK

Dr. jur. Alexander Koch

Postfach 15 01 61

53040 Bonn

Tel.: 02 28 / 8 50 86 63

Fax: 02 28 / 8 50 86 62

ak@irnik.de

WWW: <http://www.irnik.de>



Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie