Datenschutz

Einf. in die Medizinische Informatik
(Teil 4a)

Ernst Schuster
Ernst.Schuster@akh-wien.ac.at
http://www.akh-wien.ac.at/Ernst.Schuster
IMC - Institut für Medizinische Computerwissenschaften
Medizinische Bildverarbeitung und Mustererkennung

Strukturierung

- Abgrenzung
  Datensicherheit ⇔ Datenschutz
- Österreichisches Datenschutzgesetz
  (Definitionen, zulässige/unzulässige Eingriffe)
- Begleit-Grundrechte
  (weitere Rechte des Betroffenen)
- Austausch von Informationen
- Zusammenfassung

Datensicherheit

(Abgrenzung zum Datenschutz)

Hohes Maß an

- Vertraulichkeit
  (nur autorisierte Personen haben Zugriff)
- Integrität
  (aktuell, vollständig, korrekt)
- Verfügbarkeit
  (Zugang zu den Daten)

Österreichisches Datenschutzgesetz

(DSG 2000, BGBl. I Nr.136/2001)

1997: erste Fassung

2000: neues Gesetz (DSG 2000)
(eng an die EU-Richtlinien angelehnt)

- Datenschutz ist ein Menschenrecht
- Schützt alle personenbezogenen Daten
  Voraussetzung:
  - nicht zugängliche Daten
  - schutzwürdiges Interesse

Österreichisches Datenschutzgesetz
(DSG 2000)

Medizinischer Bereich

„§4 Abs. 2"

Gesundheitsdaten = sensible Daten

Österreichisches Datenschutzgesetz
(DSG 2000, BGBl. I Nr.136/2001)

Im Artikel 1

„Grundrecht auf Datenschutz"

wird das

Recht auf Geheimhaltung

in den Verfassungsrang gehoben.

Definitionen
(§ 4 Z 1 DSG 2000)

- "Daten" ("personenbezogene Daten"): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist
- "nur indirekt personenbezogen" sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann

Personenbezogene Daten

Daten über identifizierte Personen:

Name	Adresse	Geburtsdatum	sonstige Informationen
Maier	Hauptstraße 1	13.03.53	

Daten über identifizierbare Personen:

Geburtsdatum	sonstige Informationen
13.03.53	

indirekt personenbezogene Daten:

verschlüsselter Identifikator	sonstige Informationen
1394	

Personenbezug ist so verschlüsselt, daß der Verwender der Daten ohne Hilfe des Schlüsselinhabers mit vernünftigem Aufwand, insbesondere mit rechtlich zulässigen Mitteln, die Daten nicht re-identifizieren kann.

Anonymisierte Daten

sonstige Informationen

Definitionen
(§ 4 Z 2 DSG 2000)

"sensible Daten" ("besonders schutzwürdige Daten"):
Daten natürlicher Personen über ihre

- rassische und ethnische Herkunft
- politische Meinung
- Gewerkschaftszugehörigkeit
- religiöse oder philosophische Überzeugung
- Gesundheit
- Sexualleben

EINGRIFFE in das Grundrecht

zulässig
(§1 Abs 2)

unzulässig

*) Wenn ein solcher Eingriff durch eine staatliche Stelle erfolgen soll, ist dies nur aufgrund einer eigenen gesetzlichen Grundlage zulässig. Wenn sensible Daten verwendet werden sollen, darf dies nur in den Fällen des §9 DSG 2000 geschehen; (dies schließt Gesetze ein, die Eingriffe wegen wichtiger öffentlicher Interessen vorsehen).

Auftraggeber einer Datenverarbeitung
(§ 4 Z 4 DSG 2000)

Auftraggeber ist,

„ wer die Entscheidung trifft, Daten für einen bestimmten Zweck zu verarbeiten"

Dies kann sein:

- eine natürliche oder juristische Person ODER
- eine Personengemeinschaft

Sonderregelung bei Gebietskörperschaften:

- die Gebietskörperschaft selbst ODER
- das zuständige Organ der Gebietskörperschaft ODER
- der Geschäftsapparat des Organs

Datenregisternummer (DVR)

Jeder Auftraggeber einer Datenanwendung muss eine DVR-Nummer führen
(sofern es keine Ausnahme von der Meldepflicht gibt)

Eine DVR-Nummer ist eine 7-stellige Registriernummer, die vom Datenverarbeitungsregister (DVR) vergeben wird.

Datenregisternummer (DVR)

Eine DVR-Nummer muss geführt werden,

- wenn man der Meldepflicht unterliegt
- bei Übermittelungen an den Betroffenen (§25 Abs. 1 DSG 2000)

Datenverarbeitung/anwendung

(§ 4 Z 4 DSG 2000)

Eine Datenverarbeitung liegt vor, wenn zur Erreichung eines inhaltlich bestimmten Zweckes personenbezogene Daten zur Gänze oder auch nur teilweise automationsunterstützt geordnet sind.

In bestimmten Sonderfällen sind auch manuell geführte Dateien (Karteisysteme) meldepflichtig z.B. bei Gesundheitsdateien.

Meldepflicht

Grundsätzlich hat jeder Auftraggeber jede Anwendung zu melden.

Ausnahmen sind in § 17 Abs. 2 DSG 2000 aufgezählt

Ausnahmen von der Meldepflicht

- Datenanwendungen, die ausschließlich veröffentlichte Daten enthalten
  (z.B. Grundbuch, Firmenbuch, in Medien veröffentlichte Bilanzdaten)

- Anwendungen, die einer Standardanwendung entsprechen.
  Eine Standardanwendung ist wie eine Meldung beim Datenverarbeitungsregister aufgebaut, aber sie ist in einer Verordnung enthalten und ersetzt die sonst übliche Meldung.
  Bitte prüfen Sie, ob eine Standardanwendung auf Ihren Fall zutrifft, bevor Sie sich darauf berufen.
  Im Zweifelsfall können Sie beim Datenverarbeitungsregister nachfragen.

Standardanwendungen

Die geltenden Standardanwendungen sind in der Standard- und Muster-Verordnung 2000 (StMV), BGBl. II Nr. 201/2000 enthalten.

Die wichtigsten Standardanwendungen für Unternehmen sind:

- SA001 Rechnungswesen und Logistik
- SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse
- SA007 Verwaltung von Benutzerkennzeichen
- SA022 Kundenbetreuung und Marketing für eigene Zwecke

Standardanwendungen

- Für niedergelassene Ärzte:
  - SA002
    Personalverwaltung für privatrechtliche Dienstverhältnisse
  - SA024
    Patientenverwaltung und Honorarabrechnung

Meldung

an das Datenverarbeitungsregister

STANDARDANWENDUNG	keine Meldepflicht
MUSTERANWENDUNG	vereinfachte Meldung
SONSTIGE ANWENDUNG	Meldung gemäß §19 Abs 1
mit besonderem Gefährdungspotential	mit Vorabkontrolle

Vorabkontrolle von Meldungen

Bei Verarbeitung
- von sensiblen Daten
- von strafrelevanten Daten
- von Daten für Kreditinformationssysteme
- im Informationsverbundsystem

Besonderheit:
Verarbeitung darf erst aufgenommen werden wenn
- innerhalb von 2 Monaten nach Meldung Verbesserungsauftrag erfolgt oder
- nachdem Registrierung (allenfalls nach Verbesserungen) erfolgt

Meldeformulare für das Datenverarbeitungsregister:
http://www.bka.gv.at/datenschutz/

Dienstleister einer Datenverarbeitung
(§ 4 Z 5 DSG 2000)

Dienstleister ist,

„wer Daten verwendet, die ihm zur Herstellung eines Werkes überlassen wurden"

Dies kann sein:

- eine natürliche oder juristische Person
- eine Personengemeinschaft
- das Organ einer Gebietskörperschaft bzw. der Geschäftsapparat solcher Organe

Definitionen
(§ 4 Z 6, Z 7 DSG 2000)

- "Datei":
  strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind

- "Datenanwendung" (früher: "Datenverarbeitung"):
  die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung)

Definitionen
(§ 4 Z 8 DSG 2000)

- "Verwenden von Daten":
  jede Art der Handhabung von Daten einer Datenanwendung, also sowohl
  - das Verarbeiten (Z 9) von Daten als auch
  - das Übermitteln (Z 12) von Daten

Definitionen
(§ 4 Z 9 DSG 2000)

"Verarbeiten von Daten":
das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister
mit Ausnahme des Übermittelns (Z 12) von Daten

Definitionen
(§ 4 Z 10, Z 11 DSG 2000)

- "Ermitteln von Daten":
  das Erheben von Daten in der Absicht,
  sie in einer Datenanwendung zu verwenden

- "Überlassen von Daten":
  die Weitergabe von Daten vom Auftraggeber
  an einen Dienstleister

Definitionen
(§ 4 Z 12 DSG 2000)

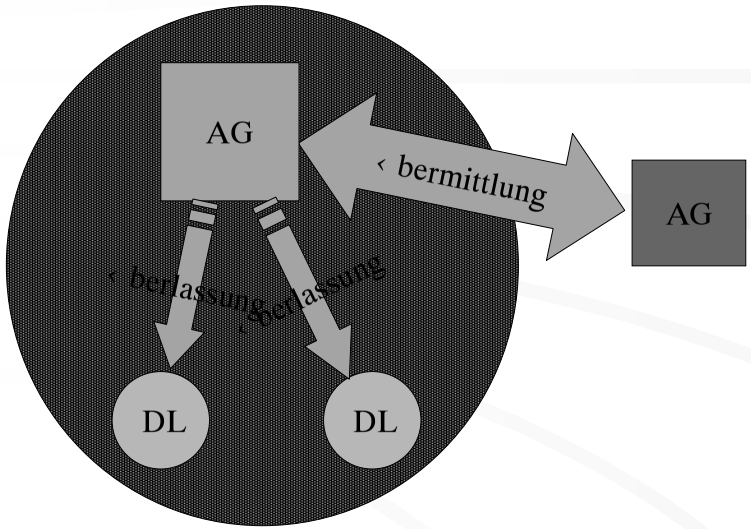
"Übermitteln von Daten":

- die Weitergabe von Daten einer Datenanwendung
  an andere Empfänger als
  - den Betroffenen
  - den Auftraggeber
  - einen Dienstleister

- insbesondere auch das Veröffentlichen solcher Daten

- die Verwendung von Daten für ein
  anderes Aufgabengebiet des Auftraggebers

Auftraggeber - Dienstleister



Definitionen
(§ 4 Z 6 DSG 2000)

"Informationsverbundsystem":

- die gemeinsame Verarbeitung von Daten
  in einer Datenanwendung durch mehrere
  Auftraggeber und
- die gemeinsame Benützung der Daten in der
  Art, daß jeder Auftraggeber auch auf jene
  Daten im System Zugriff hat, die von den
  anderen Auftraggebern dem System zur
  Verfügung gestellt wurden

Verwendung von Gesundheitsdaten

- Es bestehen keine schutzwürdigen Geheimhaltungsinteressen
- Bestehende Geheimhaltungsinteressen werden nicht verletzt
- durch Gesetz vorgesehen (z.B. Ärztegesetz)

Verwendung von Gesundheitsdaten

- § 9 Z 1:
  Der Betroffene hat die Daten veröffentlicht
- § 9 Z 2:
  Es werden nur indirekt personenbezogene Daten verwendet
- § 9 Z 6:
  mit ausdrücklicher Zustimmung des Betroffenen

  § 9 Z 10:
  Verwendung für wissenschaftliche Forschung
- § 9 Z 12:
  Verwendung zur Behandlung

Definitionen
(§ 4 Z 14 DSG 2000)

- "Zustimmung":
  die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt

§ 9 Z 12 DSG 2000

Erlaubt die Verwendung von Daten, soweit sie

„zum Zweck

- der Gesundheitsvorsorge oder
- der medizinischen Diagnostik oder
- der Gesundheitsversorgung oder –behandlung oder
- für die Verwaltung von Gesundheitsdiensten

erforderlich ist, und

die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen"

Wissenschaftliche Forschung
(§ 46 DSG 2000)

Oberster Grundsatz
(§ 46 Abs. 5 DSG 2000)

Soweit irgend möglich

nur indirekt personenbezogene

Daten verwenden

Wissenschaftliche Forschung
(Fortsetzung)

Welche Daten dürfen immer verwendet werden?

- (zulässigerweise) veröffentlichte Daten
- indirekt personenbezogene Daten
- Daten, die der Auftraggeber für einen anderen Zweck (z.B. Behandlung) zulässigerweise ermittelt hat

Wissenschaftliche Forschung
(Fortsetzung)

Alle übrigen Daten dürfen nur verwendet werden

- gemäß einer besonderen gesetzlichen Vorschrift
- mit ausdrücklicher Zustimmung des Betroffenen
- mit Genehmigung der Datenschutzkommission

Genehmigung der Datenverwendung durch die DSK

Verschafft nur Ermächtigung zur Datenübermittlung, aber keinen Anspruch darauf

- Voraussetzungen für eine Genehmigung:
  - Einholung der Zustimmung wäre unverhältnismäßiger Aufwand UND
  - öffentliches Interesse an der beantragten Verwendung UND
  - Glaubhaftmachung der fachlichen Eignung des Antragstellers

Ermittlung von Adressdaten
(§ 47 DSG 2000)

Adressdaten dürfen
zum Zweck der Befragung von Personen für Forschungsprojekte
an den Forscher übermittelt werden, wenn

- **„harmloses" Auswahlkriterium** (z.B. Wohnort , Altersklasse)
  - an der Befragung ein öffentliches Interesse besteht — ODER
  - der Betroffene der Datenweitergabe nicht widerspricht
- **sensibles Auswahlkriterium**
  - die Einholung der Zustimmung zu aufwendig ist — UND
  - die Genehmigung der Datenschutzkommission vorliegt, für die glaubhaft gemacht werden muss, dass Daten für ein bestimmtes wissenschaftliches Forschungsprojekt gebraucht werden

PRINZIPIEN
rechtmäßiger Datenverwendung

- Daten dürfen nur für einen **rechtlich zulässig**en, von vornherein definierten Zweck verwendet werden
- Sie müssen für diesen Zweck **wesentlich** sein (und nicht darüber hinaus gehen)
- Sie müssen sachlich **richtig** und, soweit nach dem Zweck der Datenverarbeitung notwendig, **aktuell** sein
- Sie dürfen **nicht länger als notwendig** gespeichert werden
- Die Datenverwendung muß insgesamt **„fair"** sein (dem Grundsatz von Treu und Glauben entsprechen)

genehmigungsfreier Datenexport
(§ 12 Abs. 3 DSG 2000)

- im Inland zulässigerweise veröffentlichte Daten
- nur indirekt personenbezogene Daten
- die Zustimmung des Betroffenen liegt vor
- Datenexport notwendig zur Erfüllung eines Vertrages mit dem Betroffenen
- in Standard- oder MusterVO vorgesehen

Genehmigungspflicht
für den Datenexport ins Ausland
(§ 12 DSG 2000)

A) **1.unabhängig** vom Datenschutzniveau im Empfängerstaat in den in §12 Abs 3 genannten Fällen	**genehmigungsfrei**
2.abhängig vom Datenschutzniveau im Empfängerstaat	
a) in einen anderen **EU-Mitgliedsstaat**	**genehmigungsfrei**
b) in einen Staat, der durch Verordnung zum Staat mit **angemessenem Datenschutz** erklärt wurde	**genehmigungsfrei**
c) in einen Staat, in dem durch Verordnung für **Teilbereiche** angemessener Datenschutz festgestellt wurde	genehmigungsfrei aber **Anzeigepflicht** an die Datenschutzkommission (Untersagung kann binnen 6 Wochen erfolgen)
B) in allen anderen Fällen	**Genehmigung** der Datenschutzkommission erforderlich

Meldepflicht für wissenschaftliche Datenanwendungen

Keine Meldepflicht bei:

- rein privaten Datenanwendungen
  (fallen nicht unter die EU-Datenschutzrichtlinie)
- Datenanwendungen, die keine direkt personenbezogenen Daten enthalten
  (kein schutzwürdiges Geheimhaltungsinteresse nach §1 DSG 2000)
- Datenanwendungen, die ausschließlich veröffentlichte Daten enthalten
  (kein schutzwürdiges Geheimhaltungsinteresse nach §1 DSG 2000)

Die Information des Betroffenen

Bei jeder Ermittlung von personenbezogenen Daten ist der Betroffenen darüber zu informieren

- für welche Datenanwendung (welchen Verarbeitungszweck) seine Daten ermittelt werden
- wer der Auftraggeber der Datenanwendung ist
- was sonst für eine „faire" Datenverwendung notwendig ist
  (z.B. Information darüber, dass die Zustimmung jederzeit widerrufen werden kann)

PFLICHTEN des Auftraggebers

- Meldepflicht
- Informationspflicht
- Richtigstellung unrichtiger Daten
- Löschung
  - unzulässig verarbeiteter Daten
  - nicht mehr gebrauchter Daten

RECHTE des Betroffenen

- Auskunft
- Widerspruch
- Richtigstellung
- Löschung

Rechtsstellung des Betroffenen

- Informationspflicht des Auftraggebers
- Besonderer Schutz vor Verwendung sensibler Daten
- Sonderregelungen für Informationsverbundsysteme
- Vorabkontrolle besonders gefährdender Datenanwendungen
- Widerspruchsrecht des Betroffenen
- Durchsetzung des Auskunftsrecht vor der Datenschutzkommission
- Schadenersatz
- Kontrollrechte der Datenschutzkommission im öffentlichen und im privaten Bereich
- Klagerecht der Datenschutzkommission vor Gericht

Austausch von Information

- Internet vs Intranet
- Handheld devices
  ⇒ überall erreichbar
  ⇒ „neues" burn-out"

Gesundheits-Telematikgesetz

www.bmsg.gv.at

Übertragungssicherheit

- Authentifizierung (Signatur)
- Vertraulichkeit (Verschlüsselung)
  (offenes Netz statt geschlossenes Netz
  ⇒ höheres Gefährdungspotential
- Veränderungssicherheit (Signatur)
- Protokollierung, Empfangsbestätigung

Gesundheits-Telematikgesetz

Informationsmanagement

- Monitoring (Sicherheitstechnologie)
- Evaluierung

Datenübertragung

- Datenschutzgesetz 2000
  §14 Datensicherheit
  - Schutz vor Zugang durch Unbefugte
  - nach technischen Möglichkeiten
  - wirtschaftlich vertretbar
- Signaturgesetz
  (elektronische statt eigenhändige Unterschrift)
  (Verschlüsselungssystem)
- MAGDA-LENA
  Richtlinien der STRING-Kommission
- Österreichische Ärztekammer-Richtlinie

Anforderungen an Befundübermittelung

- Verfolgbarkeit
- Integrierbarkeit in Patientenkartei
- Lesbarkeit
  d.h. inhaltliche Normung (HL7)
- Verwechslungsschutz
  (Pat.-ID)
- Kostenwirtschaftlichkeit

Zusammenfassung

- Datenschutz ist ein Grundrecht
- Gilt für alle Datenanwendungen
  (nicht nur EDV-gestützte)
- Rechte des Patienten
- Oberstes Prinzip
  Hochachtung vor dem Menschen

Danke

für Ihre Aufmerksamkeit