

Datenschutz

Rainer Doubrawa

Vortrag anlässlich der DV der LPPKJP Okt. 2009

Übersicht

1. Historische Grundlagen des Datenschutzes
2. Gesetzliche Grundlagen des Datenschutzes
3. Gesetzssystematik
4. Personenbezogene Daten
5. Rechte der Betroffenen
6. Der behördliche Datenschutzbeauftragte
7. Datenschutz in der LPPKJP
8. Datenschutz und Datensicherheit in der psychotherapeutischen Praxis

Danksagung

Einen Teil der folgenden Folien (besonders zu 3. bis 5.) konnte ich aus einer Fortbildungsveranstaltung des Hessischen Datenschutzbeauftragten (Herr Sobota) verwenden, wofür ich mich bedanke.

1. Historische Grundlagen des Datenschutzes

- Hippokratischer Eid (um 400 v. Chr.)
- Schutzrecht für das Briefgeheimnis (in Deutschland vor ca. 1000 J., Rabbi Gerschom ben Jehuda)
- Allgemeines preußisches Landrecht 1794: Regelung der Schweigepflicht für Ärzte
- 1970 erstes Datenschutzgesetz weltweit: in Hessen, 1971 erster Datenschutzbeauftragter
- **Volkszählungsurteil des BVerfG 1983 (Ableitung des „Rechts auf informationelle Selbstbestimmung“ aus GG Art. 1)**

2. Gesetzliche Grundlagen in Deutschland (1)

Grundgesetz (GG):

- Artikel 1: Die Würde des Menschen ist unantastbar ...
- Artikel 2: Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und ...
- Artikel 10: Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich

Gesetzliche Grundlagen (2)

- Europäische Datenschutzrichtlinie (34 Artikel)
- Bundesdatenschutzgesetz (BDSG)
- Telemediengesetz (z. B. E-Mail, Homepage)
- Sozialgesetzbuch (SGB):
 - SGB V: Übermittlung von Daten an Leistungsträger.
 - SGB X: Sozialgeheimnis

Gesetzliche Grundlagen (3)

- Bürgerliches Gesetzbuch (BGB):
Behandlungs-/Dienstvertrag (§§ 611, 328, 677)
- Strafgesetzbuch (StGB):
Schweigepflicht und Unversehrtheit der Daten (§§ 201 – 206, 303a)
- Strafprozessordnung: Zeugnisverweigerungsrecht (§ 53)
- Berufsordnung:
Datensicherheit (§ 10), Schweigepflicht (§ 11)

3. Gesetzessystematik: Wann gilt welches Gesetz ?

Bundesdatenschutzgesetz

Landesdatenschutzgesetz

bereichsspezifische Gesetze

(z. B. auch kirchliche Datenschutzgesetze bzw. –verordnungen)

Was gilt denn nun ?

Anwendungsbereich

Als erstes gilt: Subsidiaritätsgrundsatz

Spezialgesetz

- Meldegesetz
- Statistikgesetz
- Sozialgesetzbuch
- Grundbuchordnung

geht vor Allgemeingesetz

- Bundesdatenschutzgesetz
- Landesdatenschutzgesetz

Subsidiaritätsgrundsatz

Es gilt immer die **speziellere Vorschrift**:

- z.B. § 12 Grundbuchordnung: „Die Einsicht des Grundbuchs ist jedem gestattet, der ein berechtigtes Interesse darlegt.“
- oder § 34 Meldegesetz (sinngemäß): Die Meldebehörde darf Auskunft über Vor- und Familienname und Anschrift erteilen.

Nicht etwa die datenschutzfreundlichere, die engere oder die strengere Vorschrift.

Subsidiaritätsgrundsatz

Manchmal ist nur eine bestimmte Sache, z.B. die Datenübermittlung oder nur eine bestimmte Phase der Datenverarbeitung z. B. die Aufbewahrungsdauer im Spezialgesetz geregelt.

Dann gilt diese Spezialregelung und ansonsten das allgemeine Datenschutzrecht

Subsidiaritätsgrundsatz

Manchmal sind auch **alle Phasen der Datenverarbeitung** geregelt wie z.B. im Polizeigesetz (HSOG) oder im Statistikgesetz.

Dann gilt das allgemeine Datenschutzrecht nur bezüglich der verbliebenen Regelungsbereiche. Das ist meist das Kontrollrecht oder die Regelungen über die technischen und organisatorischen Maßnahmen

Anwendungsbereich

Bei Anwendung des allgemeinen
Datenschutzrechtes ist danach die
Kompetenz des Gesetzgebers zu betrachten:

Dort wo das Land die Gesetzgebungshoheit hat
gilt das Landesrecht. Ansonsten gilt
Bundesrecht

Anwendungsbereich

Bereich	Beispiel	Recht
Bund	Arbeitsverwaltung , BKA, BZRG	BDSG
Land	Landesministerien, LKA, Kommunen	HDSG
privater Bereich	Firmen, Vereine, Parteien	BDSG

Anwendungsbereich

Unabhängig von jeder Systematik kann eine gesetzliche Anwendungsregel vorgehen:

z.B. im Wassergesetz ([..\sonst.
Material\Wassergesetz.htm](#))

z.B. im Strafvollzugsgesetz ([..\Rechtsvorschriften](#))

Oder im jeweiligen Datenschutzgesetz

z.B. § 3 HDSG [..\Rechtsvorschriften\1999-HDSG.htm](#) oder

z.B. § 1 BDSG [..\Rechtsvorschriften\2003-BDSG.pdf](#)

Struktur des HDSG

1. Teil – Allgemeiner Datenschutz
 1. Abschnitt – Grundsatzregelungen
 2. Abschnitt – Rechtgrundlage der DV
 3. Rechte der Betroffenen
2. Teil - HDSB
3. Teil - Besonderer Datenschutz
4. Teil - Rechte des Landtages
5. Teil - Schlussvorschriften

Struktur des BDSG

Erster Abschnitt – Allgemeine Bestimmungen

- Zweck und Anwendungsbereich
- Technischer und organisatorischer Datenschutz
- Datenschutzbeauftragter

Zweiter Abschnitt – DV der öffentlichen Stellen

- Rechtsgrundlagen der Datenverarbeitung
- Rechte der Betroffenen
- Bundesbeauftragter für den Datenschutz

Dritter Abschnitt – DV nicht öffentlicher Stellen

- Rechtsgrundlagen der Datenverarbeitung
- Rechte der Betroffenen
- Aufsichtsbehörde

Vierter Abschnitt - Sondervorschriften

4. Definitionen

Was versteht man unter dem Begriff
personenbezogene Daten?

Personenbezogene Daten

Sind das nur : - Geburtsdatum,
 - Eheschließungsdatum,
 - Sterbedatum.

Oder sind das auch: - Name,
 - Vorname,
 - Adresse.

Personenbezogene Daten

Was ist mit

- einem Lichtbild,
- einem DNA-Muster,
- einem Blutstropfen,
- einem Mülleimer,
- einer Fensterbank?

Personenbezogene Daten

Definition in § 2 Abs. 1 HDSG

„Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.

Identisch mit § 3 Abs. 1 BDSG

Personenbezogene Daten

- Herr Meier hat einen Unfall verursacht.
- Frau Schulze ist Hauseigentümerin.
- Herr Müller wohnt in Frankfurt.
- Frau Schmidt ist krank.

Personenbezogene Daten

Die Stadt Fulda ist total verschuldet.

Die Firma Strunz AG macht hohe Gewinne.

Herr Meier, verstorben 1944, war ein
Nationalsozialist.

Personenbezogene Daten

Ein Vater von 12 Kindern aus Wiesbaden-Kloppenheim (500 Einwohner) hat im Lotto gewonnen.

Der 2,07 m große Mann aus Eschwege ist HIV-infiziert.

Sämtliche 5 Mitglieder der Familie Kreuz aus Kassel haben einen Führerschein.

Begriffsbestimmungen

Was ist eigentlich Datenverarbeitung ?

Ist das nur der technische Ablauf eines
bestimmen Verarbeitungsprozesses?

Oder ist das mehr ?

Begriffsbestimmungen

Was beinhaltet Datenverarbeitung ?

Definition in § 2 Abs. 2 HDSG

„Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten...“

Einzelne Phasen der Datenverarbeitung sind das Erheben, Speichern, Übermitteln, Sperren oder Löschen von Daten.

Begriffsbestimmungen

Was ist eigentlich Datenverarbeitung ?

Es gibt noch die sonstige Nutzung, die in den Bereich der Datenverarbeitung, aber nicht in die genannten Phasen fällt.

Nicht identisch und im Gegensatz zu § 3 Abs. 3 bis 5 BDSG

Datenverarbeitung

Ist es Datenverarbeitung

- Wenn ein Bürger ein Antragsformular ausfüllt ?
- Wenn Sie eine Aktennotiz zerreißen und in den Papierkorb werfen?
- Wenn Sie von einer anderen Behörde Akten anfordern?
- Wenn Sie eine Aktenanforderung erfüllen?

Datenverarbeitung

Ist es Datenverarbeitung

- Wenn Sie einen „Fall“ mit Kollegen besprechen ?
- Wenn Sie aus dem Fenster gucken?
- Wenn der Polizeibeamte am Straßenrand den Verkehr beobachtet.
- Wenn eine Videokamera läuft ?

Datenschutz im Bereich Medizin und Psychotherapie

bedeutet kurzgefasst:

**Konsequente Anwendung
der Schweigepflicht bzw. des
Patientengeheimnisses**

5. Rechte der Betroffenen

- Auskunft und Benachrichtigung.
- Akteneinsicht.
- Prüfung auf Unverhältnismäßigkeit.
- Einsicht in das Verfahrensverzeichnis.
- Berichtigung, Sperrung, Löschung.
- Schadensersatz.
- Anrufung des Datenschutzbeauftragten.

Auskunft - § 18

Das Auskunftsrecht nach § 18 Abs. 3 umfasst:

- Art und Inhalt gespeicherter Daten.
- Zweck und Rechtsgrundlage der Datenverarbeitung.
- Herkunft und Empfänger (soweit gespeichert) der Daten.

Akteneinsicht - § 18

Es gilt ein Akteneinsichtsrecht nach Abs. 5

Ausnahme:

Bei der Verbindung mit Daten Dritter oder geheimhaltungsbedürftigen Informationen muss eine Trennung erfolgen. Ist dies unmöglich oder unverhältnismäßig aufwendig wird nur Auskunft erteilt.

Recht auf Einzelfallabwägung

§ 7 Abs. 5 HDSG

Auch eine rechtmäßige DV kann den Betroffenen besonders belasten.

Solch eine Belastung muss mit dem Interesse an der DV im Einzelfall abgewogen werden.

Vorbemerkung Nr. 45 und Artikel 14 der EU-Richtlinie.

Einsicht in das Verfahrensverzeichnis

§ 6 Abs. 2 HDSG

Jeder darf das Verfahrensverzeichnis einsehen.

Ausnahmen: gegebenenfalls Ziffern 7, 8, 11

Weitere Ausnahmen:

Verfahren des Verfassungsschutzes, der
Polizei, der Staatsanwaltschaften sowie der
Steuerfahndung.

Berichtigung, Sperrung, Löschung

- Berichtigung - § 19 Abs. 1 HDSG
- Sperrung - § 19 Abs. 2 HDSG
- Löschung - § 19 Abs. 3 HDSG

Schadenersatz

§ 20 HDSG

Schadenersatzpflicht bis zu 250.000 €.

Hat bislang kaum praktische Bedeutung.

Anrufung des Datenschutzbeauftragten

- Jeder Betroffene kann sich an den HDSB wenden - § 28 Abs. 1
- Öffentliche Bedienstete brauchen keinen Dienstweg einzuhalten - § 28 Abs. 2

6. Der behördliche Datenschutzbeauftragte

nach § 5 des Hessischen
Datenschutzgesetzes (HDSG)

Aufgaben des behördlichen Datenschutzbeauftragten

- ▶ Hinwirken auf die Einhaltung der DS-Vorschriften
- ▶ Unterrichtung der Beschäftigten über DS-Vorschriften
- ▶ Unterstützung der Behörde bei Erstellung des Verfahrensverzeichnisses sowie bei den technischen und organisatorischen Maßnahmen zur Durchführung des DS
- ▶ Führung des Verfahrensverzeichnisses und Bereithaltung für die Einsicht
- ▶ Überprüfung der Vorabkontrolle bei Einsatz oder Änderung von Verfahren automatisierter Verarbeitung von personenbezogenen Daten

Stellung des behördlichen Datenschutzbeauftragten

- ▶ Die Behörde hat einen DS-Beauftragte (schriftlich) zu bestellen (und einen Stellvertreter)
- ▶ Der behördliche DS-Beauftragte untersteht unmittelbar der Leitung der Behörde
- ▶ Er hat das Recht, sich jederzeit schriftlich oder mündlich an die Leitung zu wenden – ohne Einhaltung eines Dienstwegs
- ▶ Ihm obliegt die unabhängige Überwachung der Einhaltung des Datenschutzes – er ist weisungsfrei tätig
- ▶ Dienststellen haben DS-Beauftragten alle Informationen zur Verfügung zu stellen, die für die Aufgabenwahrung benötigt werden
- ▶ Interessenkonflikte sind zu vermeiden (d. h. z. B. Dienststellenleiter oder EDV-Leiter dürften nicht als DS-Beauftragte bestellt werden)
- ▶ Der DS-Beauftragte hat keine Exekutivfunktion. Er kann Hinweise geben, aber keine Anweisungen

Das Verzeichensverzeichnis

(Verfahren zur automatisierten Verarbeitung personenbezogener Daten - nach § 6 HDSG)

In dem Verzeichnis ist folgendes festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle
2. Zweckbestimmung und Rechtsgrundlage der DV
3. Art der gespeicherten Daten
4. Kreis der Betroffenen
5. Art der rglm. übermittelten Daten, deren Empfänger sowie die Art und Herkunft rglm. empfangener Daten

Verfahrensverzeichnis Forts.

6. Zugriffsberechtigte Personen oder Personengruppen
7. Die technischen und organisatorischen Maßnahmen (nach § 10, z. B. Zutrittskontrolle, Benutzerkontrolle, Zugangskontrolle, DV-Kontrolle, Verantwortlichkeitskontrolle u. a.)
8. Die Technik des Verfahrens
9. Fristen für die Löschung (§ 19 Abs. 3)
10. Eine beabsichtigte Datenübermittlung (§ 17)
11. Das begründete Ergebnis der Untersuchung (§ 7 Abs. 6, Satz 3: Ist das Recht des einzelnen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, geschützt?)

Verfahrensverzeichnis – Beispiele (LPPKJP)

- Mitgliederverwaltung (einschl. Beitragsbemessung)
- Personaldatenverwaltung (wenn über EDV)
- Temporäre Verfahrensverzeichnisse: z. B. bei Mitgliedererhebungen (etwa freiwilliger Meldebogen), Umfragen o. ä.

Wichtig dabei: das **Prinzip der Datensparsamkeit** beachten!

7. Datenschutz in der LPPKJP (1)

- Sichere Aufbewahrung von Personalakten mit Schutz vor unbefugtem Zugang
- Sicherheit der Datenübertragung per Telefon oder Telefax
- Sicherheit (Ort, Zugang, Wartung usw.) des Servers
- Katastrophenschutz (Wasser, Feuer, Einbruch u. ä.)
- Sicherheit der Datenübertragung im LAN (oder WLAN)
- Datenschutz und –sicherheit an den Computern (Passwortschutz, sichere Passwörter, Regelung Zugangsberechtigung, passwortgeschützte Bildschirmschoner usw.)
- Sicherung von USB-Schnittstellen
- Sachgerechte Datenspeicherung (verschlüsselt)
- Regelmäßige (tgl.) Datensicherung (auf externen Medien)
- Zugangsgesicherte Verwahrung der externen Medien (Wo?)

Besonders wichtiges Beispiel: E-Mail-Kommunikation

- Virenschutz und Firewall
- Der unverschlüsselte Versand von Nachrichten mit personenbezogenen Daten, die der Schweigepflicht unterliegen, stellt eine unbefugte Offenbarung dar!
- Solche E-Mails sind zu verschlüsseln (z. B. mit PGP-Software)
- Bei mehreren Empfängern einer Mail deren Adressen nicht für alle sichtbar eingeben (Bcc-Funktion nutzen)

Datenschutz in der LPPKJP (2)

- Software für die EDV-Dokumentation muss Schutz vor nachträglicher Veränderung der Daten bieten
- Beachtung der Aufbewahrungsfristen:
 - bei längeren Fristen (10 J. und mehr) auf Haltbarkeit der Speichermedien achten
 - bei Bedarf auf aktuell gebräuchliche Speichermedien kopieren
 - gespeicherte Daten müssen jederzeit lesbar bleiben (auf Software und Speichermedien achten)

Datenschutz in der LPPKJP (3)

- Sachgerechte Entsorgung von Akten (z. B. Papier schreddern nach Sicherheitsstufe 3 (DIN 32757))
- Zeit- und sachgerechte Löschung von personenbezogenen Daten auf den Rechnern und dem Server (mehrfaches Überschreiben, z. B. mit Programmen wie BCWipe oder Eraser)
- Defekte Festplatten auch physikalisch zerstören

8. Datenschutz in der psychotherapeutischen Praxis (1)

Die hinsichtlich der Kammer genannten Punkte gelten natürlich entsprechend auch für die psychotherapeutische Praxis

Weitere Aspekte – darüber hinaus:

- Kein unbeaufsichtigter Zugang zur Praxis
- Diskretion bei Empfang, Verabschiedung, Telefonaten mit PatientInnen
- Schutz von Akten, Karteikarten, Monitoren vor Einsicht durch Unbefugte

Datenschutz in der psychotherapeutischen Praxis (2)

- Patientengespräche in geschlossenen Räumen, geschützt vor neugierigen Augen und Ohren
- Patientenrechte: z. B. Einsicht in die objektiven Aufzeichnungen in der Patientenakte, schriftliche Einwilligung des Pat., wenn Privatrechnungen über Verrechnungsstellen in Auftrag gegeben werden
- Bei Anfragen von Dritten: können Berichte oder Bescheinigungen nicht evt. besser vom Pat. selbst weitergegeben werden?

Datenschutz in der psychotherapeutischen Praxis (3)

- **Schweigepflichtentbindung** seitens des Patienten – ist erforderlich, soweit nicht eine gesetzliche Offenbarungsbefugnis (z. B. gegenüber GKV oder MDK) oder ein rechtfertigender Notstand gegeben ist:
z. B. gegenüber dem Versorgungsamt, einer privaten Versicherung, bei Forschungszwecken, gegenüber Angehörigen

Datenschutz in der psychotherapeutischen Praxis (4)

- Die **Schweigepflichtentbindung** muss folgende **Angaben** enthalten:
 - Wer** entbindet: Name, Geb.-Dat. und Anschrift des Pat.,
 - Wem** gilt sie: Name des Therapeuten
 - Wofür**: Zweck der Datenweitergabe
 - Was**: um welche Daten genau geht es
 - An wen** gerichtet: Bezeichnung der Stelle, des Arztes usw.
 - Wie lange** gültig: einmalige oder wiederholte Offenbarung?
Evt. Hinweis auf Möglichkeit des Widerrufs
 - Datum** und **Unterschrift** des Patienten

Datenschutz in der psychotherapeutischen Praxis (5)

- Sachgerechte Entsorgung von Akten und sichere Löschung von Dateien
- Datenschutz und –sicherheit bei PC-Reparaturen
- Datenschutz und –sicherheit bei Praxisumzug
- Sichere Passwörter (Kombination von Buchstaben, Groß- und Kleinschreibung, Zahlen, Sonderzeichen, rglm. Wechsel)
- Sicherung von Notebooks (z. B. Fingerabdruck-Scanner, Alarmsicherung)
- Sicheres Laufwerk (mit Steganos Security Suite)
- eGK und Heilberufsausweis

Literaturhinweise

- Jochen NUNGESSER: Hessisches Datenschutzgesetz – unter Berücksichtigung der EG-Datenschutzrichtlinie. Mainz 2001 (2. Aufl.)
- C. BAKE, B. BLOBEL, P. MÜNCH (Hrsg.): Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen. Heidelberg 2009 (3. Aufl.)
- A. HÖPKEN, H. NEUMANN. Datenschutz in der Arztpraxis. Ein Leitfaden für den Umgang mit Patientendaten. Heidelberg 2008 (2. Aufl.)

Gesundheitsrecht in der Praxis

Höpken/Neumann

Datenschutz in der Arztpraxis

Ein Leitfaden für den Umgang
mit Patientendaten

2., überarbeitete Auflage



C. F. Müller
MedizinRecht.de

Web-Adressen

- Hessischer Datenschutzbeauftragter:
www.datenschutz.hessen.de
- Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein:
www.datenschutzzentrum.de
- Bundesamt für Sicherheit in der
Informationstechnik:
www.bsi.bund.de

Vielen Dank für Ihre
Aufmerksamkeit!