

Chaos Computer Club Stuttgart

Datenschutz – Dein gutes Recht

Victoria Polzer

Datenschutz - was ist das überhaupt?

- Ziel ist nicht primär der Schutz von Daten, sondern

den Einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird

(§ 1 Abs. 1 Bundesdatenschutzgesetz)

Personenbezogene Daten

- *Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person* (§ 3 Abs. 1 BDSG)
→ alle Informationen, die man mir zuordnen kann
- also z.B. Name, Anschrift, Geburtsdatum, Beruf, Aussehen; mein Kontostand, Informationen darüber, wann und mit wem ich telefoniert habe, die Tatsache, daß ich ein Händi besitze usw.
- auch "belanglose" und veröffentlichte Daten
- *bestimmbar*: Person kann durch Zusatzinformationen ermittelt werden (z.B. Autokennzeichen, Kontonummer auf dem Bibliotheksausweis, IP-Adresse eines Rechners)

Persönlichkeitsrecht

- "Allgemeines Persönlichkeitsrecht" geschützt durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs.1 GG
→ freie Entfaltung der Persönlichkeit, inhaltliche Bestimmung (Verstärkung) von der Garantie der Menschenwürde her
- sog. "unbenanntes Freiheitsrecht"
- Integrität der Persönlichkeit in geistig-seelischer Beziehung (nicht ihr Tun, sondern ihr Sein)
→ **Datenschutz ist Grundrechtsschutz!**

Persönlichkeitsrecht (2)

- Persönlichkeitsrecht umfaßt z.B.
 - den sozialen Geltungsanspruch (persönliche Ehre)
 - Anspruch auf Resozialisierung von Strafgefangenen
- in unserem Zusammenhang wichtig:
 - Recht auf Selbstdarstellung in der Öffentlichkeit
 - Recht am eigenen Wort und am eigenen Bild
 - Recht auf Gegendarstellung
 - das Recht, vor Gericht nicht gegen sich selbst aussagen zu müssen
 - Schutz der Privatsphäre ("in Ruhe gelassen werden")
 - **übergreifend: informationelle Selbstbestimmung**

Informationelles Selbstbestimmungsrecht

- Begriff aus den 70er Jahren
- Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 definiert Umfang und Schranken:
 - Herleitung aus Art. 2 Abs. 1 iV, 1 Abs. 1 GG
→ freie Entfaltung der Persönlichkeit setzt Schutz der personenbezogenen Daten voraus
 - Recht gewährleistet die *Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*
 - Einschränkung nur in überwiegendem Allgemeininteresse

Wo ist das Problem?

- Zusammenhang Entfaltung der Persönlichkeit ↔ Verarbeitung personenbezogener Daten?
- deutlich bei Tagbüchern, Telefongespräch mit der besten Freundin, Briefen, E-Mails, bei dem was ich meiner Wohnung sage und tue
- und sonst – Daten, die sowieso jeder kennen kann wie Name, Adresse, Telefonnummer und "belanglose" Daten wie Einkaufsgewohnheiten und Hobbies?

Automatisierte Datenverarbeitung

- EDV ermöglicht Speicherung riesiger Datenmengen
- elektronische Datenbestände können schnell & gezielt nach bestimmten Kriterien durchsucht & gruppiert werden
- Verknüpfung verschiedener Datenbestände ist möglich, dadurch Vergleich, Abgleich, Erstellen von Persönlichkeitsbildern, "Profilen" → "gläserner Mensch"
- auch "belanglose" Daten können Verknüpfungen ermöglichen und zu einem Steinchen im Mosaik werden z.B. Cookies im Internet-Browser
- Informationen werden verkürzt, ohne Kontext gespeichert, so daß ein verzerrtes Bild der Person entsteht

Habe ich was zu verbergen?

- Sollen meine "Jugendsünden" ewig im Bundeszentralregister und im Führungszeugnis gespeichert bleiben?
- Kann mein Nachbar erfahren, daß ich AIDS habe?
- Darf ein Arbeitgeber mich bei der Bewerbung nach meiner Gewerkschafts- oder Parteizugehörigkeit fragen?
- Muß ich beim Abschluß einer Lebensversicherung einen Gen-Test auf Risikofaktoren vornehmen lassen?
- Kriege ich einen Händi-Vertrag, wenn die Firma weiß, daß ich öfter meine Stromrechnung zu spät zahle?

→ **Gefahr von wirtschaftlicher, sozialer oder politischer Diskriminierung**

Gesellschaftliche Bedeutung

Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.

(Bundesverfassungsgericht, Entscheidungen, Band 65, S. 154)

Welches Gesetz schützt mich denn nun?

- datenschutzrechtliche Bestimmungen in vielen verschiedenen Gesetzen verstreut
- Regel: bereichsspezifische Vorschrift (z.B. für Gesundheitsdaten, Versicherungsverträge, Schulen, Hochschulen, Telekommunikation ...) hat Vorrang, allgemeine Datenschutzgesetze gelten nur, wenn es keine spezielle Vorschrift für die Situation gibt
- Hinweis: wer erhebt welche Daten wozu, z.B.
 - Krankenkasse → Gesundheitsdaten → SGB
 - T-Online → Abrechnung Internet-Zugang → TKG & TDSV
 - Uni → Noten u.a. bei Immatrikulation → LHG & HSDV

Spezialgesetzlich geregelte Bereiche

(Auswahl)

Steuer- & Abgabenrecht

Sozialrecht

Arbeitsrecht

Gewerbe- & Handelsrecht

Schul- & Hochschulrecht

Vertragsrecht

Verwaltungsverfahrensrecht

Pass- & Melderecht

Polizei- & Sicherheitsrecht

Medien- & Kommunikationsrecht

Bundesdatenschutzgesetz (BDSG)

- unterschiedliche Vorschriften für öffentliche Stellen und Private → **Gesetz hat daher mehrere Teile**
- ein Teil für Bundesbehörden (& u.U. Landesbehörden)
- ein Teil für Firmen, Vereinen, Privatleute
 - regelt z.B. Umgang mit Kundendaten, Werbung etc.
 - begegnet häufig, Vorbild für andere Regelungen
- Inhalt der Landesdatenschutzgesetze ist weitgehend deckungsgleich mit dem BDSG (etwas anders formuliert, andere Reihenfolge, einige Ergänzungen oder Auslassungen)

Prinzipien der gesetzlichen Regelung

- Regelungen in den einzelnen Gesetzen unterschiedlich, aber nach denselben Prinzipien:
 - "Verbot mit Erlaubnisvorbehalt"
 - Erforderlichkeitsprinzip & Zweckbindung
 - Transparenz gegenüber dem Betroffenen
 - Korrektur- & Abwehrrechte des Betroffenen
 - Verpflichtung zur Datensicherung durch technische & organisatorische Maßnahmen
 - interne und externe Aufsicht & Kontrolle
 - Sanktionsmaßnahmen
- im Einzelfall sehr starke Abweichungen (z.B. für Polizeien, Geheimdienste, Staatsanwaltschaft)

Was nicht erlaubt ist, ist verboten

- **"Verbot mit Erlaubnisvorbehalt"** heißt: wenn es keine ausdrückliche Erlaubnis für genau diesen Schritt der Datenverarbeitung gibt, ist er unzulässig (verboten)
- **Erlaubnis kann sein**
 - 1) Rechtsvorschrift
 - 2) Einwilligung des Betroffenen
- **Folgen** unzulässiger Datenverarbeitung: Anspruch auf Löschung, Verwertungsverbote (z.B. vor Gericht), evtl. Schadensersatz

Wer nichts weiß, kann sich nicht wehren

- **Transparenz gegenüber dem Betroffenen:**
ich muß wissen, wer welche Daten über mich erhebt, sonst kann ich mich dagegen nicht wehren
- **darum:**
 - Datenerhebung grundsätzlich beim Betroffenen
 - bei dieser Datenerhebung Unterrichtung über Zweck, evtl. Weitergabe an Dritte, Kennzeichnung von freiwilligen & Pflichtangaben, Nennung der Rechtsgrundlage und der Folgen einer Verweigerung von Angaben und – wichtig! – Identität der speichernden Stelle
- Ich muß diese Hinweise aber auch lesen!

Auskunftsrecht

- Werden Daten bei Dritten erhoben, muß der Betroffene (eigentlich) informiert werden
 - macht allerdings kaum jemand, bringt wenig
 - zu viele Ausnahmen, Kontrolle schwierig
- wichtig statt dessen: Auskunftsrecht – Anfrage nach (vermutlich) erfolgter Speicherung
- "unabdingbares Recht" – kann nicht durch vertragliche Regelung o.ä. ausgeschlossen werden
 - durch Gesetz schon, problematisch z.B.: Geheimdienste

Sag mir, was Du über mich weißt...

- Auskunftsrecht gegenüber Firmen: § 34 BDSG
- man kann Auskunft verlangen über
 - die zu seiner Person gespeicherten Daten (im Detail, also welches Geburtsdatum, welcher Kontostand, welche nicht bezahlte Rechnung etc.)
 - deren Herkunft
 - den Zweck der Speicherung
 - Dritte, an die diese Daten weitergegeben wurden
- ein paar Ausnahmen (z.B. Herkunft & Empfänger nur, wenn "Wahrung des Geschäftsinteresses" nicht überwiegt)
- Mustertexte für Auskunftsanfragen gibt's im Internet

Was man nicht braucht, darf man nicht haben

- **Erforderlichkeitsprinzip & Zweckbindung:** man darf nur die Daten verarbeiten, die man für einen genau bestimmten (und legitimen) Zweck benötigt, und man darf sie nur zu diesem Zweck verwenden
- viele Unternehmen verlangen mehr Daten als nötig
 - nachfragen, das Unternehmen ist verpflichtet, die Frage zu beantworten!
 - ggf. Antwort verweigern – nicht erforderliche Daten muß man nicht angeben (und der Vertragsschluß dürfte an fehlender E-Mailadresse o.ä. in der Regel nicht scheitern)
 - z.B. Geburtsdatum oder E-Mail *und* Adresse oft unnötig

Auf in den Kampf...

- **Korrektur- & Abwehrrechte:**
Berichtigung, Sperrung, Löschung
- Berichtigung: Pflicht des Unternehmens, wenn es falsche Informationen über mich speichert
- Löschung:
 - wenn Daten verbotenerweise erhoben wurden
 - bei besonders sensiblen Daten (z.B. Religion, ethnische Herkunft, Gesundheit, politische Meinung), deren Richtigkeit nicht bewiesen werden kann
 - Daten für den ursprünglichen Zweck nicht mehr benötigt

Sperrung von Daten

- Sperrung heißt: Daten dürfen für den normalen Gebrauch nicht mehr verwendet werden, werden aber auch nicht gelöscht
- z.B. durch Kennzeichnung des Datensatzes in einer Datenbank oder Tabelle
- Zwischenlösung, solange Richtigkeit der Daten umstritten
- Ersatzlösung, wenn Daten nicht mehr verwendet werden dürfen, aber Löschung nicht erlaubt/möglich
 - z.B. gesetzliche Aufbewahrungspflichten für Buchhaltung

Ich sage NEIN ...

- häufig kann man einer bestimmten Nutzung oder der Weitergabe seiner Daten **widersprechen**
- Vertragsformulare haben oft entsprechende Felder zum Ankreuzen (genau lesen!)
- sonst kann man auch auf dem Vertragsformular handschriftlich widersprechen ("keine Nutzung oder Übermittlung meiner Daten zu Werbezwecken" o.ä.)
- oder später schriftlich widersprechen (z.B. wenn man namentlich adressierte Werbung bekommt)
- zusätzlich Eintrag in "Robinsonlisten"

Wenn's hart auf hart kommt ...

- erster Ansprechpartner: Datenschutzbeauftragter der Stelle, die meine Daten verarbeitet
- sonst die zuständige Aufsichtsbehörde
 - die zuständige Stelle zu finden ist nicht so ganz einfach, im Zweifelsfall einfach beim Landesdatenschutzbeauftragten nachfragen oder direkt an ihn schreiben, der leitet den Brief dann weiter
 - kann ggf. ein Bußgeld verhängen
- Unterlassungs- und/oder Schadensersatzklage
- Strafantrag
(nur bei Vorsatz und Bereicherungsabsicht)

Datenschutz – Do it Yourself

- **sich informieren** – Datenschutzerklärung, AGBs u.a. "Kleingedruckte" aufmerksam lesen und bei Zweifeln nachfragen, was wozu mit den Daten gemacht wird
- **sich schützen** – nicht jedes Formular ausfüllen, Nutzung seiner Daten widersprechen, keine Rabattkarten o.ä. verwenden, mehr bar bezahlen, seinen Computer (z.B. den Web-Browser) sicher konfigurieren, E-Mails verschlüsseln...
- **sich wehren** – seine Rechte aus dem BDSG (u.a. Gesetzen) wahrnehmen: der Nutzung und Weitergabe zu Werbezwecken widersprechen, Auskunft verlangen, ggf. auf Berichtigung, Sperrung oder Löschung bestehen, Datenschutzbeauftragte und Aufsichtsbehörden einschalten

Soll ich jetzt wirklich anfangen, Auskunftsanfragen, Widerspruchserklärungen und Beschwerdebriefe zu schreiben?

- JA!
- Firmen verzichten nicht von allein auf Daten, man muß sie davon überzeugen, daß ihre Kunden Datenschutz wollen – oder sie eben zur Einhaltung der Vorschriften zwingen.
- Datenschutzbehörden brauchen Eingaben der Bürger, um auf Probleme aufmerksam zu werden.
- Man sollte seine Rechte in Anspruch nehmen, sonst gibt es sie womöglich irgendwann nicht mehr.