8 Sicherheitsziel: Personenbezogene Daten informationelles Selbstbestimmungsrecht

8.1 Gegenstand des Datenschutzes

Der Schutz vor dem Missbrauch seiner Daten wird vom Schutz der "Persönlichkeit" allgemein und ihrer "Privatsphäre" abgeleitet. Das allgemeine Persönlichkeitsrecht ist im Grundgesetz kodifiziert:

Art. 1 Abs 1 GG: "Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen, ist Verpflichtung aller staatlichen Gewalt."

Art. 2 Abs. 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."

Der einzelne soll grundsätzlich selbst entscheiden können, wie er sich Dritten und der Öffentlichkeit gegenüber darstellen will, ob und inwieweit von Dritten über sein Persönlichkeitsbild verfügt werden kann.

Daher hat der einzelne -unter Beachtung der Rechte anderer- das Recht auf Selbstbestimmung über die eigene "soziale Rolle".

Dieses Recht auf Selbstdarstellung wird auch als **informationelles Selbstbestimmungsrecht**. ("Recht am eigenen Datum") bezeichnet.

Dieser Begriff zielt ergänzend auf die Kontrollrechte über die Verarbeitung der ihn betreffenden Informationen.

Gegenstand des Datenschutz ist also

- der Schutz des informationellen Selbstbestimmungsrechts des einzelnen und mithin
- der Schutz seiner Freiheit, über die eigenen Daten grundsätzlich selbst bestimmen zu dürfen und
- die rechtsstaatliche Absicherung dieses Anspruchs.

8.2 Sensibilität von Daten

Nicht alle personenbezogenen Daten sind gleich sensibel.

Eine Orientierung gibt das nachfolgende **Schutzstufenkonzept**, das beim Hamburger Datenschutzbeauftragten entwickelt wurde:

Stufe A:
personenbezogene Daten, deren Missbrauch keine besondere Beeinträchtigung erwarten lässt, z.B.

- Adressangaben (Name, Anschrift, Tel.-Nr.)
- Berufs-, Branchen-, oder Geschäftsbezeichnungen.

Stufe B:
personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann, z.B.

- Daten über Mietverhältnisse,
- Daten über Geschäftsbeziehungen.

Stufe C:
personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann bzw. die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (insbesondere die Daten, die in §28 Abs. 2 Nr. 1 BDSG aufgeführt sind), die sich auf

- gesundheitliche Verhältnisse,
- strafbare Handlungen,
- Ordnungswidrigkeiten,
- religiöse oder politische Anschauungen,
- arbeitsrechtliche Rechtsverhältnisse beziehen.

Stufe D:
personenbezogene Daten, deren Missbrauch für den Betroffenen Gefahren für Leib und Leben bedeuten, z.B.

- Adressen von polizeilichen V-Leuten,
- Adressen von Zeugen in bestimmten Strafverfahren.

Letztlich bestimmt jedoch die Einschätzung (und Erfahrung) des einzelnen, wie sensibel die einzelnen Daten sind.
Z.B. wird ein Opfer von Telefonterror die Information über seine Telefonnummer für sensibler halten als die Information über seine Miete.

Achtung:

Werden die Daten intensiver EDV-Auswertung unterzogen, so gibt es überhaupt kein belangloses Datum mehr, da durch Kombination vieler wenig sensibler Daten sensiblere Daten entstehen können (z.B. bei der Re-Identifikation).

8.3 Eckpfeiler des Datenschutzes

8.3.1 Das Urteil des Bundesverfassungsgerichts zum Volkzählungsgesetz 1983

Das Bundesverfassungsgericht hat -im sog. Volkszählungsurteil 1983 (1 BvR 209/83 u.a.)- das Recht auf **informationelle Selbstbestimmung** aus den Grundrechten der Verfassung abgeleitet.

Leitsätze zum Urteil:

"1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss.
   Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten.

   Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymisierter Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind.
   Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden.
   Der Informationserhebung und -verarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen.

4. Das Erhebungsprogramm des Volkszählungsgesetzes 1983 (§2 Nr. 1 bis 7, §§ 3 bis 5) führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der Persönlichkeit; es entspricht auch den Geboten der Normenklarheit und der Verhältnismäßigkeit.
   Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung.

5. Die in §9 Abs. 1 bis 3 VZG 1983 vorgesehenen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht.
   Die Weitergabe zu wissenschaftlichen Zwecken (§9 Abs. 4 VZG 1983) ist mit dem Grundgesetz vereinbar."

In vielen Bundesländern (Berlin, Brandenburg, Bremen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Saarland, Sachsen-Anhalt, Thüringen) ist der Datenschutz inzwischen in den Landesverfassungen verankert worden.

8.3.2 Das Bundesdatenschutzgesetz

Das **Bundesdatenschutzgesetz** (BDSG vom 20.12.1990 mit späteren Änderungen) regelt die

- **Erhebung** (*collection*),
- **Verarbeitung** (*processing*) und
- **Nutzung** (*use*)

personenbezogener Daten (*personal data*)

- für die öffentlichen Stellen (soweit es ein Landesdatenschutzgesetz gibt, gilt dieses für die öffentlichen Stellen des Landes) und
- für die nicht-öffentlichen Stellen (§ 1(2)).

Das **Erheben** personenbezogener Daten ist durch öffentliche Stellen **zulässig** (*admissible*), wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist (§13 (1)).

Personenbezogene Daten sind beim Betroffenen zu erheben (§13 (2)) (*data collection from the data subject*). Ihm ist der Erhebungszweck (*purpose*) anzugeben sowie die Rechtsvorschrift, die ihn zur Auskunft verpflichtet bzw. er ist auf die Freiwilligkeit hinzuweisen (§13 (3)-(4)).

Eine **Verarbeitung** personenbezogener Daten und deren **Nutzung** ist nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt (*consent*) hat (§4, Details in §14, §§28-29).
Verarbeiten ist das Speichern (*storage*), Verändern (*modification*), Übermitteln (*communication*), Sperren (*blocking*) und Löschen (*erasure*) (§ 3 (5)).

Ein **Bundesbeauftragter für den Datenschutz** (*Federal Commissioner for Data Protection*)

- kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Datenschutzvorschriften (§24) und
- beanstandet Verstöße dagegen (§25). Insbesondere
- erstattet er zweijährlich dem Deutschen Bundestag einen Tätigkeitsbericht und
- führt ein von jedem einsehbares Dateienregister (*register of data files*) über alle automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden.

Der Betroffene hat unabdingbare Rechte auf

- **Auskunft** (*provision of information to the data subject*) insbesondere über die zu seiner Person gespeicherten Daten und den Zweck der Speicherung (§§ 19, 34),
- **Berichtigung** unrichtiger Daten,
- **Löschung** insbesondere unzulässig gespeicherter oder nicht mehr erforderlicher Daten und
- **Sperrung** –statt Löschung– insbesondere falls der Löschung Aufbewahrungsfristen oder schutzwürdige Interessen des Betroffenen entgegenstehen (§§ 20, 35).

Von nicht-öffentlichen Stellen ist der Betroffene bei erstmaliger Speicherung seiner Daten i.a. zu **benachrichtigen** (*notification*) (§33).

Jeder kann den Bundesbeauftragten für den Datenschutz anrufen, wenn er sich durch öffentliche Stellen des Bundes in seinen Datenschutzrechten verletzt fühlt.

Alle Stellen, die personenbezogene Daten verarbeiten, haben die **technischen und organisatorischen Maßnahmen** zu treffen, um die Vorschriften des BDSG umzusetzen (§9, insbesondere Anlage zu §9).

Nicht-öffentliche Stellen, die mindestens fünf Arbeitnehmer mit der automatisierten Verarbeitung (oder zwanzig Arbeitnehmer mit der Verarbeitung) personenbezogener Daten beschäftigen, müssen einen **Beauftragten für den Datenschutz** bestellen (§36), der die Durchführung der Datenschutzvorschriften sicherstellen soll.
Die **Aufsichtsbehörde** (*supervisory authority*) überprüft im Einzelfall bei nicht-öffentlichen Stellen die Ausführung der Datenschutzvorschriften (§38).

Am 24.10.95 hat der Europäische Rat der **Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr** zugestimmt (**Europäische Datenschutzrichtlinie**).

Damit müssen die Mitgliedstaaten der Europäischen Union (u.a. die Bundesrepublik Deutschland) bis zum 24.10.98 ihr nationales Datenschutzrecht auf einem hohen Niveau angleichen und den gegenwärtigen Schutz der Bürger verbessern.

Die Novellierung des Bundesdatenschutzgesetzes wurde erst am 14.06.00 vom Bundeskabinett verabschiedet. Die Umsetzung im Gesetzgebungsverfahren dauert an.

Aus der **Datenschutzkonvention des Europarates** [CoE 81]:

Datenschutzziele

the personal data shall be
- obtained and processed fairly and lawfully,
- stored for specified and legitimate purposes and not used in a way incompatible with those purposes,
- adequate, relevant and not excessive in relation to the purposes for which they are stored,
- accurate and, where necessary, kept up to date,
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

8.3.3 Grundsätze des Datenschutzes (im öffentlichen Bereich):

- **Gebot der Normenklarheit**: Der Bürger muss aus einer gesetzlichen Regelung klar erkennen können, zu welchem konkreten Zweck seine Daten verwendet werden.

- **Gebot der Erforderlichkeit und Zweckbestimmtheit**: Staatliche Maßnahmen dürfen nicht weiter gehen, als es zur Verfolgung des jeweiligen Zweckes unbedingt erforderlich ist (Übermaßverbot). Eine Ausnahme gilt für die Statistik. (Forschung umstritten)

- **Prinzip der Verhältnismäßigkeit**: Der Umfang der Daten ist je nach Aufgabe einzuschränken und die Beeinträchtigung der Betroffenen so gering wie möglich zu halten.

- **Grundsatz der informationellen Gewaltenteilung**: Jede öffentliche Stelle darf nur speichern, was sie zur Erfüllung ihrer Aufgaben braucht. Datenweitergabe darf nur kontrolliert (unter Einhaltung der Übermittlungsvorschriften) geschehen.

- **Grundsatz der Durchschaubarkeit der Datenverarbeitung**: Der Bürger muss Kenntnis darüber erlangen können, wer wo über welche seiner personenbezogenen Daten in welcher Weise und zu welchem Zweck verfügt (Effektivität des Rechtsschutzes).

  Kontrollinstanzen, **Kontrolleinrichtungen**, **Auskunftsrecht**.

Im privaten Bereich kommen diese Grundsätze zumindest mittelbar zur Geltung.

Insbesondere folgende Punkte werden zur Umsetzung dieses Rechts als unverzichtbar angesehen:

1. **Transparenz der Datenverarbeitung**: Ein Bürger kann sein Recht auf informationelle Selbstbestimmung nur wahrnehmen, wenn er weiß, "wer, wo über welche seiner personenbezogenen Daten, in welcher Weise und zu welchem Zweck verfügt";
   was über ihn gespeichert wird und welche Konsequenzen das haben kann.

1a. **Datenerhebung beim Betroffenen**, d.h. der Betroffene (und nicht jemand anders) wird nach seinen Daten gefragt.
1b. **Auskunftsrecht des Betroffenen** bzgl. der über ihn gespeicherten Daten sowie Herkunft und Empfänger der Daten und des Zweckes der Speicherung.
1c. **Dateienregister** erlaubt Überblick, wer Daten welcher Art speichert und wem regelmäßig weitergibt.

2. **Zweckbindung der Daten**, d.h. eine Datenverarbeitung ist nur für den Zweck zulässig, für den die Daten erhoben worden sind.

2a. **Rollentrennung**: U.a. Institutionen dürfen nicht unbegrenzt zusammenarbeiten.

3. **Nachprüfbarkeit durch Datenschutzinstitutionen**: Bundesbeauftragter für Datenschutz, Aufsichtsbehörde; entsprechende Landesbehörden.

4. **Nachberichtspflicht** (Einmal übermittelte Daten sollen berichtigt werden, wenn Sie danach unrichtig geworden sind. "Unrichtige Daten dürfen kein Eigenleben führen." (LDSG S-H 26.9.91))