Rechtliche Regelungen zu Datenschutz und Datensicherheit

Das Grundgesetz der Bundesrepublik Deutschland

Das Grundgesetz bildet die **rechtliche und politische Grundordnung** der Bundesrepublik Deutschland. Alle anderen Rechtsnormen müssen sich den hier verankerten **Grundrechten** beugen.

Auszug aus dem Grundgesetz der Bundesrepublik Deutschland, Stand: 09/2017

Artikel 1: (1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt...

Artikel 2: (1) 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. (2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden...

Der Schutz im Umgang mit Daten war bis zum Jahr 1983 (noch) nicht im Grundgesetz festgeschrieben. Deshalb prägte das Bundesverfassungsgericht in dem *Volkszählungsurteil* vom 15. 12. 1983 den Begriff *informationelle Selbstbestimmung*.

Informationelle Selbstbestimmung

Die Begründung ist in dem Urteil des Bundesverfassungsgerichts formuliert:
„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht 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.“
(*Das Bundesverfassungsgericht; BVerfG, 1 BvR 209/83 vom 15. 12. 1983 unter C II 1 a*)

- Informationelle Selbstbestimmung bedeutet also, dass der Betroffenen über die Verwendung seiner persönlichen Daten bestimmen kann. Eingriffe in dieses Recht sind nur auf gesetzlicher Grundlage möglich, wobei der Betroffene darüber zu informieren ist.

Das Strafgesetzbuch und die Strafprozessordnung

- Im **Strafgesetzbuch** (StGB) werden die Voraussetzungen und Rechtsfolgen strafbaren Handelns in Deutschland geregelt („materielles Strafrecht“).
- Durch die **Strafprozessordnung** werden die Verfahren zur Durchführung von Strafverfahren geregelt („formelles Strafrecht“).

Das deutsche Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)

Das *Zweite Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft* trat zum 01. 01. 2008 in Kraft. Danach besitzt der Urheber das alleinige Recht, darüber zu entscheiden, was mit seinen Werken geschieht – egal, ob es sich um Musik, Bilder, Grafiken, Fotos, Filme, Texte, Software, wissenschaftliche Erkenntnisse oder technische Erfindungen handelt.

In der Regel überträgt der Urheber gegen Geld die Nutzungsrechte an Rechteverwerter wie Musiklabels, Verlage oder Filmverleihe (*vgl. Lerninhalte 1.7-04–Rechtliche Grundlagen*).

Datenschutzgesetze

Datenschutzgrundverordnung der Europäischen Union

In der **Datenschutz-Grundverordnung** (DSGVO) werden Grundsätze für die Speicherung und Verarbeitung personenbezogener Daten innerhalb der EU festgelegt.
Das betrifft z. B. den Schutz vor einer Beeinträchtigung des Rechts auf **informationelle Selbstbestimmung** und die Gewährleistung des freien Datenverkehrs innerhalb des Europäischen Binnenmarktes.
Die Datenschutz-Grundverordnung gilt auch für Organisationen und Unternehmen außerhalb der EU, die Daten von EU-Bürgern speichern und verarbeiten:

Datenschutz-Grundverordnung vom 04.05.2016; Inkrafttreten: 24.05.2016; Anzuwenden ab 25.05.2018
Artikel 1 (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Einzelne Klauseln der DSGVO können in nationalen Gesetzen der Mitgliedsstaaten konkreter geregelt oder eingeschränkt werden.

Bundesdatenschutzgesetz

In dem **Bundesdatenschutzgesetz** (BDSG) wird der Datenschutz für den **privaten Bereich** (Privatpersonen und Wirtschaftsunternehmen) und für die **Bundesbehörden** geregelt. Das BDSG musste auf Grund der neu eingeführten DSGVO überarbeitet werden:

Bundesdatenschutzgesetz Letzte Neufassung vom 30.06.2017; Inkrafttreten: 25.05.2018
§ 1 (1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch
1. öffentliche Stellen des Bundes,
2 öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
a) Bundesrecht ausführen oder
b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.
Für nichtöffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Bayerisches Datenschutzgesetz

Die **Datenschutzgesetze der Länder** wurden zur Regelung des Datenschutzes in Landes- und Kommunalbehörden erlassen:

Bayerisches Datenschutzgesetz (BayDSG) vom 23.07.1993; zuletzt geändert am 24.07.2017:
Artikel 1 Zweck des Gesetzes
Zweck dieses Gesetzes ist es, die einzelnen davor zu schützen, daß sie bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen in unzulässiger Weise in ihrem Persönlichkeitsrecht beeinträchtigt werden.

Die Grundsätze für die Speicherung und Verarbeitung personenbezogener Daten und ihre Konkretisierung werden auf der folgenden Seite zusammengefasst.

Grundsätze für die Speicherung und Verarbeitung personenbezogener Daten in Deutschland

Die Einhaltung der Datenschutzgesetze wird durch **Datenschutzbeauftragte** kontrolliert:

- Der Bundesbeauftragte für den Datenschutz hat die Aufsicht über die öffentlichen Stellen des Bundes sowie über Unternehmen der Telekommunikations- und Postdienstleistungsbranche.
- Alle anderen privaten Unternehmen werden von Datenschutzaufsichtsbehörden kontrolliert, die beim Landesdatenschutzbeauftragten oder bei Landesbehörden angesiedelt sind.
- Die Landesbehörden unterliegen der Kontrolle durch die Landesdatenschutzbeauftragten.

International anerkannte Datenschutzprinzipien, die in den deutschen Datenschutzgesetzen gewährleistet werden, sind:

- Das Prinzip der **Zulässigkeit und Rechtmäßigkeit** der Erhebung und Verarbeitung von Daten betrifft die Einhaltung der Grundrechte (Würde des Menschen, Persönlichkeitsrecht).
- Nach dem Prinzip der **Richtigkeit** müssen zu verarbeitende Daten überprüft werden.
- Prinzip der **Zweckgebundenheit**: Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden und nicht zu lange gespeichert werden.
- Das Prinzip der **Verhältnismäßigkeit** bezeichnet den Schutz vor übermäßigen Eingriffen als Merkmal eines Rechtsstaates: Ein Eingriff in die Grundrechte muss *zweckgebunden* sein und daraufhin geprüft werden, ob er *geeignet*, *erforderlich* und *angemessen* ist.
- Das Prinzip der **Transparenz** besagt, dass jeder wissen soll, wer welche Daten über ihn verarbeitet und beinhaltet auch ein **Auskunftsrecht** des Betroffenen.
- Das Prinzip der **individuellen Mitsprache** und des Zugriffsrechts für die Betroffenen.
- Prinzip der **Nichtdiskriminierung**: Besonders sensible Daten, die zu einer Diskriminierung des Betroffenen führen können, dürfen nur unter bestimmten Voraussetzungen verarbeitet werden (z. B. ethnische Zugehörigkeit oder weltanschauliche Überzeugungen).
- Nach dem Prinzip der **Sicherheit** müssen technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes ergriffen werden, z. B. dass nur berechtigte Personen auf die Daten zugreifen können.
- Prinzip der **Haftung**: Betroffene können evtl. Schadenersatzforderungen geltend machen.
- Prinzip einer unabhängigen **Datenschutzaufsicht** und gesetzlicher Sanktionen.
- Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

Zusammengefasst betreffen die wichtigsten **Prinzipien** des Datenschutzes den Grundsatz der Verhältnismäßigkeit:

- **Datensparsamkeit** und **Datenvermeidung**
- **Zweckbindung**
- **Erforderlichkeit**: Es sollen nur die Daten erhoben werden, die für die Erfüllung der Aufgabe unbedingt nötig sind.
  Daten sind also zu löschen, sobald sie nicht mehr benötigt werden.

Über allen weiteren Maßnahmen steht der **Grundsatz des Verbots mit Erlaubnisvorbehalt**:

- Die Erhebung, Speicherung und Verarbeitung personenbezogener Daten ist so lange verboten, bis
  - der Gesetzgeber dies zulässt oder
  - der Betroffene ausdrücklich einwilligt.

A Bearbeite das Arbeitsblatt 11: Rechtliche Regelungen

Internationale Datenschutzstandards

- In Deutschland gibt es seit den 1970er-Jahren Datenschutzgesetze. Das traf aber noch zu Beginn des 21. Jahrhunderts für viele Länder *nicht* zu.
  Z. B. in den USA zum Beispiel gab es im Jahr 2017 (noch) kein Datenschutzgesetz.
- Der Standort des Servers, über den ein Internetauftritt gehostet wird, ist nicht ohne weiteres zu erkennen (vgl. Lerninhalte 2.5.1–03, S. 5: Die OSI-Schichten 5 bis 7).
- Noch bedenklicher ist die Tatsache, dass automatisierte Abläufe bei der Verarbeitung und Übertragung von Daten in Netzwerken fast nicht nachvollziehbar sind: Einmal abgeschickt, hat der Benutzer keinen Zugriff mehr auf seine Daten.

➢ Terrorismus ist international, aber Computernetzwerke ebenfalls!

***SWIFT** steht für eine internationale Genossenschaft der Geldinstitute mit Sitz in Belgien, die den Nachrichtenverkehr zwischen über 8000 Geldinstituten in mehr als 200 Ländern abwickelt. Im November 2005 betrugen die Geldtransfers etwa 4,8 Billionen Euro täglich.*
(Der SWIFT/BIC-Code einer Überweisung kennzeichnet die internationale Bankleitzahl.)

*Seit den Terroranschlägen am 11. September 2001 in den USA wurden von Servern der SWIFT in den USA Daten über Finanztransaktionen an US-amerikanische Behörden übermittelt. Betroffene wurden nicht informiert. **Publik wurde dies erst 2006**.*

Nach selten einmütiger, heftiger Kritik aus der europäischen Öffentlichkeit, Presse, Politik und Wirtschaft verlegte SWIFT die Server in die Schweiz und die Niederlande.
Ab Januar 2010 konnten die Amerikaner nicht mehr auf die Informationen zugreifen.

Daraufhin wurde zwischen den USA und europäischen Innenministern das so genannte SWIFT-Abkommen ausgehandelt. Danach wären bei internationalen Banküberweisungen der Name, Betrag und Empfänger an die USA geliefert worden. Nach Überzeugung vieler Europaabgeordneter und Datenschützer hätte das aber europäische Datenschutzstandards verletzt.
Am 11.02.2010 lehnte das Europaparlament dieses Abkommen zunächst ab. Am 28.06.2010 wurde das nachverhandelte Abkommen unterzeichnet, nach dem die Auswertung der europäischen Daten im amerikanischen Finanzministerium von einem EU-Beamten überwacht wird.
Im Zusammenhang mit der NSA-Spähaffäre wurde aber bekannt, dass amerikanische Geheimdienste weiterhin das SWIFT-Netzwerk ausspionierten. Daraufhin verlangte das Europäische Parlament am 23.10.2013, das SWIFT-Abkommen mit den Vereinigten Staaten auszusetzen.

In den USA ist der Datenschutz auch im Jahr 2017 nicht durch Gesetze oder andere Vorschriften geregelt. Im Gegenteil, der Zugriff auf private Daten wird gesellschaftlich häufig akzeptiert, solange es sich nicht um Daten amerikanischer Staatsbürger handelt.

Entsprechend ist die rechtliche Situation zu internationalen Datentransfers kompliziert:

➢ Nationale Bestimmungen zum Datenschutz sind weltweit unterschiedlich.
  International sind Verstöße gegen Datenschutzbestimmungen nur schwer nachvollziehbar.

Im Fall des SWIFT-Abkommens argumentierten Vertreter von Wirtschaftsunternehmen, mit den erhobenen Daten könne Wirtschaftsspionage betrieben werden. Obwohl hier also ein großes wirtschaftliches Interesse vorhanden war, wurde nicht geklärt, ob das Vorgehen der amerikanischen Behörden rechtlich korrekt war.

➢ Der Einzelne kann sich gegen den Missbrauch seiner Daten letztlich nur dadurch wehren, dass er darauf achtet,
  - möglichst wenig Daten zu hinterlassen,
  - genau hinzuschauen, wohin er Daten sendet
  - bzw. welche Daten eventuell über ihn erhoben werden könnten.

A Bearbeite das Arbeitsblatt 12: Zusammenfassende Aufgaben zu Datenschutz und Datensicherheit