



**Datenschutzrecht**

Ass. jur. Joachim Bokor, LL.M.

Hintergründe (historische und international)  
Grundlagen (Begriffsbestimmungen)  
zulässige Datenverarbeitung nach BDSG

01  
Hintergründe

Historisch, international, europäisch, Verfassung

## 1.1 Historischer Hintergrund

**1890** „The Right to Privacy“ Warren and Brandeis Harvard Law Review IV, S. 193 ff

Vor Right to Privacy: Albert v Strange und Right to be let alone

Im engeren Sinne ein „Right to be let alone“ bzw. Recht am eigenen Bild und presserechtlich

Ansätze über informationelle Selbstbestimmung

1960er Diskussion über Misstände in der Kreditwirtschaft (Banken fragen in der Nachbarschaft)

Alan F. Westin: (1967) “The claim of individuals... to determine for themselves when, how, and to what extent information about them is communicated to others.”

## 1.1 Historischer Hintergrund

**1890** „The Right to Privacy“ Warren and Brandeis Harvard Law Review IV, S. 193 ff

**1970** Hessisches Datenschutzgesetz

ab 1970: Datenschutz wird zum politischen Bürgerrechtsthema.

Schutz vor Missbrauch / Verlust der Daten

1973: Idee des „Rechts auf informationelle Selbstbestimmung“ entsteht,

ab Mitte der 1970er: Verrechtlichung und Institutionalisierung des Datenschutzes, Einrichtung der Landesdatenschutzbeauftragten.

## 1.1 Historischer Hintergrund

**1890** „The Right to Privacy“ Warren and Brandeis Harvard Law Review IV, S. 193 ff

**1970** Hessisches Datenschutzgesetz

**1977** Bundesdatenschutzgesetz (BDSG)

"Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken."

## 1.1 Historischer Hintergrund

**1890** „The Right to Privacy“ Warren and Brandeis Harvard Law Review IV, S. 193 ff

**1970** Hessisches Datenschutzgesetz

**1977** Bundesdatenschutzgesetz (BDSG)

**1983** Volkszählungsurteil, BVerfGE 65, 1

Anlass Gesetz zur Volkszählung, Melderegisterabgleich Vermischung administrativer und statistischer Funktionen

1983: Volkszählungsurteil, „Recht auf informationelle Selbstbestimmung“ als Grundrecht. (Ausprägung des allgemeinen Persönlichkeitsrechts)

Später näher

## 1.1 Historischer Hintergrund

**1890** „The Right to Privacy“ Warren and Brandeis Harvard Law Review IV, S. 193 ff

**1970** Hessisches Datenschutzgesetz

**1977** Bundesdatenschutzgesetz (BDSG)

**1983** Volkszählungsurteil, BVerfGE 65, 1

**1991** 1. BDSG Novelle

1991 Reaktion auf Volkszählungsurteil

3. abMitterder 1990:TechnisierungdesDatenschutzes:„Privacy- Enhancing-Technologies“ (PET), Reaktion auf Internet-Risiken.

4. ab2000:Prozeßorientierung und Ökonomisierung des Datenschutzes, Entwicklung eines Datenschutz-Gütesiegels und –Audits: „Privacy sells“.  
Technisch: Erste Entwicklungen von Konzepten und Applikationen nutzer-kontrollierten Identitätsmanagement und Credentials,

## 1.1 Historischer Hintergrund

**1890** „The Right to Privacy“ Warren and Brandeis Harvard Law Review IV, S. 193 ff

**1970** Hessisches Datenschutzgesetz

**1977** Bundesdatenschutzgesetz (BDSG)

**1983** Volkszählungsurteil, BVerfGE 65, 1

**1991** 1. BDSG Novelle

**2001** 2. BDSG Novelle

Auch: Schutz vor unzureichenden Wirklichkeitsmodellen bzw. Kontextproblemen

Novelle 2001 Umsetzung der RL 95/46/EG

Februar 2008 BVerfG: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

## 1.1 Historischer Hintergrund

**1890** „The Right to Privacy“ Warren and Brandeis Harvard Law Review IV, S. 193 ff

**1970** Hessisches Datenschutzgesetz

**1977** Bundesdatenschutzgesetz (BDSG)

**1983** Volkszählungsurteil, BVerfGE 65, 1

**1991** 1. BDSG Novelle

**2001** 2. BDSG Novelle

**2009** 3 Änderungen des BDSG

ab 2006 neue Leitlinie: „Datenschutz in die Prozesse!“

Integration von Datenschutz in Common Criteria, BSI Grundschutz, EurPrise Gütesiegel

Reaktion auf mehrere „Skandale“ Kunden- u Arbeitnehmerdaten

## 1.2 Internationaler Hintergrund

### **EMRK (1950)**

#### **Artikel 8** – Recht auf Achtung des Privat- und Familienlebens

1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

EMRK (Europarat) in D Rang einfachen (+) Gs, 1950 kein DS iEs, Kontrolle durch EGMR, weite Interpretation für Eingriffsgrund, formal eng.

## 1.2 Internationaler Hintergrund

**EMRK**  
**OECD**

Art. 8 „Recht auf Achtung des Privatlebens und der Korrespondenz“ 1950  
„Leitlinien für den Schutz des Persönlichkeitsbereichs und den  
grenzüberschreitenden Verkehr personenbezogener Daten“, Dok. C (80) 58

OECD DS kein Verkehrshindernis, 1980, Selbstregulierung der Beteiligten

## 1.2 Internationaler Hintergrund

<b>EMRK</b>	Art. 8 „Recht auf Achtung des Privatlebens und der Korrespondenz“, 1950
<b>OECD</b>	„Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“, Dok. C (80) 58
<b>Europarat</b>	„Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Datenschutz Konvention, Straßburger Vertrag)“ 1985

DS Konvention, völkerrechtlich bindend, nur automatische Verarbeitung Daten natürlicher Personen, Grundsätze aktuell, freier Vk zwischen Staaten als „Ausgleich“

## 1.2 Internationaler Hintergrund

<b>EMRK</b>	Art. 8 „Recht auf Achtung des Privatlebens und der Korrespondenz“, 1950
<b>OECD</b>	„Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“, Dok. C (80) 58
<b>Europarat</b>	„Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Datenschutz Konvention, Straßburger Vertrag)“ 1985
<b>UN</b>	„Richtlinie zur Regelung von automatisierten personenbezogenen Dateien“, 14.12.1990 (A/RES/45/95)

Empfehlende UN Richtlinie, sehr allgemein, nicht verbindlich,

### 1.3 Europarechtliche Grundlagen

Richtlinien:

- **95/46/EG:** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSRL)
- **02/19/EG, 02/21/EG und 02/58/EG:** über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation
- **03/31/EG:** E-Commerce
- **06/24/EG:** über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher Kommunikationsnetze erzeugt oder verarbeitet werden und zu Änderung der Richtlinie 2002/58/EG

Alle in nationales Recht umgesetzt

„Verarbeitung“ weiter gefasst

Vorabkontrolle in sensiblen Bereichen

Angemessenes Datenschutzniveau u Übermittlung in Drittstaaten; safe haven und codes of conduct

jetzt Verfassungsrechtliche Grundlagen, hier evtl. Exkurs allgemeine Grundrechtslehre

#### 1.4 Verfassungsrechtliche Grundlagen Volkszählungsurteil

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden. [...] Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergeleitet 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 Handlungs- 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.**“

BVerfGE 65, 1, 43

Kein belangloses Datum mehr (Aufgabe der Sphärentheorie)

Informationelle Gewaltenteilung

Die automatisierte Datenverarbeitung birgt die Möglichkeit der Auswertung und Verknüpfung von Datenbeständen, die an verschiedenen Orten vorhanden sind: keine belanglosen Informationen

- Möglich damit eine vollständige Offenlegung der Privatsphäre der Bürger

- [Es] wird der Schutz des Einzelnen gegen unbegrenzte Erhebung [...] seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG 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:

- Recht auf informationelle Selbstbestimmung

## 1.4 Verfassungsrechtliche Grundlagen Grundgesetz

### **Art 1**

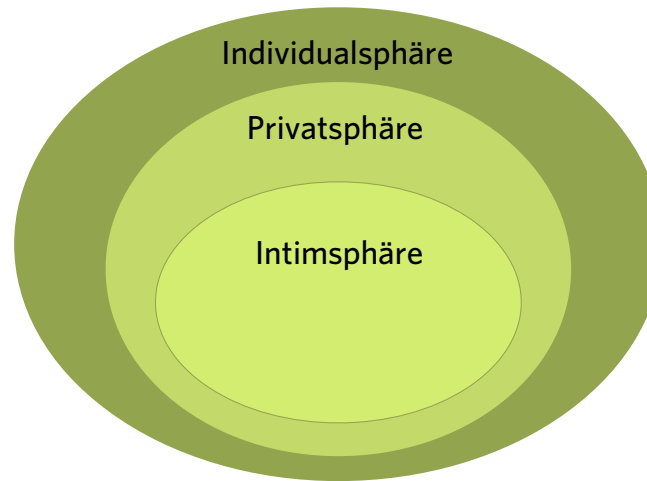
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

[...]

### **Art 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.

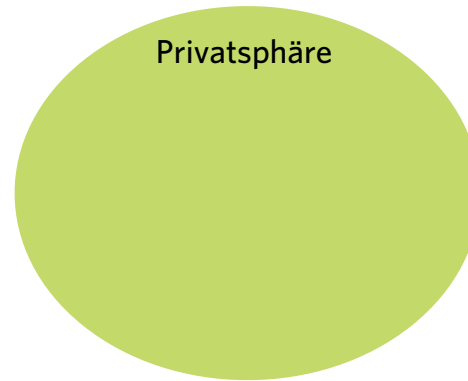
[...]



Individual-/Sozial-/Öffentlichkeitssphäre: weitgehend ungeschützt (eg auf professioneller Internetseite veröffentlichte Info)

Privatsphäre: weitgehend geschützt

Intimsphäre: absolut geschützter Bereich privater Lebensgestaltung (eg Tagebücher)



Urteile zum großen Lauschangriff und Rasterfahndung ~angelsächs „privacy“

In 4 Bereiche geteilt: persönliche Unversehrtheit, Identitätsmerkmale, Persönlichkeitsentfaltung, Kernbereich privater Lebensgestaltung

=> Zuordnung bestimmt Mglkt staatlichen Eingriffs,

Persönlichkeitsentfaltung: Differenziert nach Intensität des Eingriffs und Gemeinschaftsbezogenheit des jeweiligen Datums (eg Religionsausübung, Versammlungs-/Berufsfreiheit)

==> DS = Schutz der Persönlichkeitssphäre bei rollenspezifischer Betrachtung

## 1.4 Verfassungsrechtliche Grundlagen weitere Rechte

- Artikel 3 GG – Allgemeine Gleichbehandlung
- Artikel 4 GG – Glaubens- und Gewissensfreiheit (Besonderer Schutz von Angaben über religiöse Überzeugungen)
- Artikel 5 GG – Meinungsfreiheit
- Artikel 8 – Versammlungsfreiheit
- Artikel 9 – Vereinigungsfreiheit
- Artikel 10 – Brief-, Post- und Fernmeldegeheimnis (§ 88 TKG)
- Artikel 13 – Unverletzlichkeit der Wohnung
- § 12 BGB – Recht am eigenen Namen
- § 2 UrhG – Urheberschutz
- § 22 KUG – Recht am eigenen Bild
- §§ 201 ff. StGB – Schutz des persönlichen Lebens- und Geheimbereichs
- § 17 UWG – Betriebs- und Geschäftsgeheimnisse
- ...

Nahezu alle GrdRe können Relevanz haben, bzw. werden vom RaiS und spezialgesetzlichen Regelungen flankiert


## 1.5 Recht auf informationelle Selbstbestimmung



- Selbstbestimmung
- Erforderlichkeitsgrundsatz
- Gesetzesvorbehalt
- Normenklarheit und Bestimmtheit
- Zweckbindung und organisatorisch-technische Schutzvorkehrungen
- Transparenz

Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe oder Verwendung seiner persönlichen Daten zu entscheiden.

- Recht auf informationelle Selbstbestimmung zählt zu den Grundvoraussetzungen einer freien Entfaltung der Persönlichkeit.

- Fundamentale Voraussetzung für eine moderne Demokratie:

  Verhinderung eines Anpassungs- bzw. Rechtfertigungsdrucks

  Erhalt der räumlichen Freiheit

  Erhalt der Teilnahmemöglichkeit am politischen Willensbildungsprozess für den einzelnen Bürger

Wirkung unter Privaten?

Als objektive Werteordnung entfalten die Grundrechte auch Wirkung im Verhältnis von Privaten untereinander:

Mittelbare Drittwirkung der Grundrechte   Ausstrahlung über Allgemeinklauseln

Wirkung des RIS unter Privaten?

RIS als Grundrecht ist Teil einer objektiven Werteordnung, die die gesamte Rechtsordnung durchdringen:

Mittelbare Drittwirkung: Einfluss auf das Verhältnis Privater zueinander.

Wirkung unter Privaten?  
Eingriffsmöglichkeiten?

Inhaltliche Anforderung: Überwiegende Allgemeininteressen -> Einschränkung nur im überwiegenden Allgemeininteresse

• Formale Anforderung: Gesetz -> Überwiegende Allgemeininteressen müssen Gegenstand einer sich ausdrücklich auf sie und ihre Folgen beziehenden gesetzlichen Regelung geworden sein.

## 02 GRUNDLAGEN

Anwendungsbereiche welche Gesetze sind wann einschlägig? Lokal und materiell. Definitionen der einzelnen Begriffe.  
evtl. Exkurs Bundes / Landesrecht

## 2.1 ANWENDUNGSBEREICH BDSG

### Bundesdatenschutzgesetz (BDSG)

#### § 1 Zweck und Anwendungsbereich des Gesetzes

[...]

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung 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,

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

2

BDSG gilt in den Fällen der Abs. 2-4 §1  
zu stellende Frage: wer ist Datenverarbeitende Stelle,  
in welchem Bereich werden die Daten verarbeitet (Vorrang des Spezialgesetzes)  
BDSG überhaupt anwendbar?

## 2.1 ANWENDUNGSBEREICH

### LDSG

## Landes DSG(e) - BbgDSG

### § 2 Anwendungsbereich

(1) Dieses Gesetz gilt für die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbände unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen (öffentliche Stellen), soweit diese personenbezogene Daten verarbeiten. Für die Gerichte sowie für die Behörden der Staatsanwaltschaft gilt dieses Gesetz, soweit sie Verwaltungsaufgaben wahrnehmen; darüber hinaus gelten für die Behörden der Staatsanwaltschaft, soweit sie keine Verwaltungsaufgaben wahrnehmen nur die Vorschriften des Abschnittes 2 dieses Gesetzes. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben einer öffentlichen Stelle des Landes wahr, ist sie insoweit öffentliche Stelle im Sinne des Gesetzes.

(1a) Der Landtag, seine Gremien, seine Mitglieder, die Fraktionen sowie deren Verwaltungen und deren Beschäftigte unterliegen mit Ausnahme des § 31 nicht den Bestimmungen dieses Gesetzes, soweit sie zur Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Der Landtag erlässt insoweit unter Berücksichtigung seiner verfassungsrechtlichen Stellung und der Grundsätze dieses Gesetzes eine Datenschutzordnung.

(2) Von den Vorschriften dieses Gesetzes gelten die §§ 7a, 8, 10a, 21, 23 und 25 bis 30 dieses Gesetzes, soweit

1. wirtschaftliche Unternehmen der Gemeinden oder Gemeindeverbände ohne eigene Rechtspersönlichkeit (Eigenbetriebe),
2. öffentliche Einrichtungen, die entsprechend den Vorschriften über Eigenbetriebe geführt werden,
3. Landesbetriebe,
4. der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbänden unterstehende juristische

Personen

des öffentlichen Rechts, die am Wettbewerb teilnehmen, personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Im Übrigen sind mit Ausnahme der §§ 4d bis 4g und des § 38 die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anzuwenden.

(3) Die Vorschriften dieses Gesetzes gehen denen eines brandenburgischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden. Im Übrigen gehen besondere Rechtsvorschriften, die auf die Verarbeitung personenbezogener Daten anzuwenden sind, den Vorschriften dieses Gesetzes vor.

## 2.1 ANWENDUNGSBEREICH SUBSIDIARITÄT

Bundesdatenschutzgesetz (BDSG)

### **§1 Zweck und Anwendungsbereich des Gesetzes**

[...]

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, **gehen sie den Vorschriften dieses Gesetzes vor**. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

[...]

Andere Vorschriften, letzte Folie letzte Stunde, gehen vor, wenn spezieller

## 2.1 ANWENDUNGSBEREICH SUBSIDIARITÄT

Landes DSG(e) - BbgDSG

§ 2 Anwendungsbereich

[...]

(3) Die Vorschriften dieses Gesetzes gehen denen eines brandenburgischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden. Im Übrigen **gehen** besondere Rechtsvorschriften, die auf die Verarbeitung personenbezogener Daten anzuwenden sind, den Vorschriften dieses Gesetzes **vor**.

Parallele Regelung im LDSG

## 2. Einfachgesetzliche Grundlagen

TKG, TMG  
SGB  
Polizeigesetze und StPO  
KURhG

Landesgesetze z.B. Archivgesetze  
Tarifverträge, Betriebsvereinbarungen

Wiederholungsfragen

Was war das erste deutsche Datenschutzgesetz?

1970 Hessen

Welches Urteil des Bundesverfassungsgerichtes von 1983 hatte grundlegende Bedeutung für den Datenschutz in Deutschland? Warum?

Volkszählungsurteil (Verfassungsbeschwerde gegen Volkszählungsgesetz 1983)  
Schaffung des Rechts auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 1 Abs. 1 und 2 Abs. 1 GG

Welchen Inhalt hat das Recht auf informationelle Selbstbestimmung?

Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe oder Verwendung seiner persönlichen Daten zu entscheiden.

- Recht auf informationelle Selbstbestimmung zählt zu den Grundvoraussetzungen einer freien Entfaltung der Persönlichkeit.
- Fundamentale Voraussetzung für eine moderne Demokratie:
  - Verhinderung eines Anpassungs- bzw. Rechtfertigungsdrucks
  - Erhalt der räumlichen Freiheit
  - Erhalt der Teilnahmemöglichkeit am politischen Willensbildungsprozess für den einzelnen Bürger

## 2. BDSG

1. Abschnitt: Allgemeine und gemeinsame Bestimmungen
  - u.a. Zweck, Anwendungsbereich, Begriffsbestimmungen
2. Abschnitt: Datenverarbeitung öffentlicher Stellen
  1. Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung
  2. Unterabschnitt: Rechte des Betroffenen
  3. Unterabschnitt: Bundesbeauftragter für Datenschutz und IF
3. Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen
  1. Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung
  2. Unterabschnitt: Rechte des Betroffenen
  3. Unterabschnitt: Aufsichtsbehörde
4. Abschnitt: Sonder-, Schluss-, Übergangsvorschriften
  - u.a. Bußgeld- und Strafvorschriften

## 2. BDSG

### Zweck

#### § 1 Abs. 1 BDSG

Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Zielsetzung des BDSG

- Technikregulierung, Schutzgesetz, Eingriffsgesetz

Schutz des Persönlichkeitsrechts

## 2.1 ANWENDUNGSBEREICH

### BDSG

### Bundesdatenschutzgesetz (BDSG)

§ 1 Abs. 2:

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung 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,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Entscheidend für örtliche Anwendung Abs. 2, BDSG Bundeseinrichtungen und nicht-öffentliche Stellen

## 2.1 ANWENDUNGSBEREICH

### BbgDSG

### Landes DSG(e) - BbgDSG

#### § 2 Anwendungsbereich

(1) Dieses Gesetz gilt für die Behörden, Einrichtungen und sonstigen öffentlichen Stellen **des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbände unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen (öffentliche Stellen)**, soweit diese personenbezogene Daten verarbeiten. Für die Gerichte sowie für die Behörden der Staatsanwaltschaft gilt dieses Gesetz, soweit sie Verwaltungsaufgaben wahrnehmen; darüber hinaus gelten für die Behörden der Staatsanwaltschaft, soweit sie keine Verwaltungsaufgaben wahrnehmen nur die Vorschriften des Abschnittes 2 dieses Gesetzes. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben einer öffentlichen Stelle des Landes wahr, ist sie insoweit öffentliche Stelle im Sinne des Gesetzes.  
[...]

7

LDSG nur für öffentliche Stellen -> nicht öffentliche Stellen immer BDSG

Art 30 GG

Die Ausübung der staatlichen Befugnisse und die Erfüllung der staatlichen Aufgaben ist Sache der Länder, soweit dieses Grundgesetz keine andere Regelung trifft oder zuläßt.

## 2.1 ANWENDUNGSBEREICH

### BDSG

### Bundesdatenschutzgesetz (BDSG)

§ 1 Abs. 2:

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung 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,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

8

„öffentliche Stellen“ <-> „nicht öffentliche Stelle“ Problem Grenzfälle und Eigenbetriebe

Unterscheidung notwendig für Abschnitte 2 und 3 d BDSG

Ausnahme für persönliche/familiäre Tätigkeiten

- wenn keine bereichsspezifische Sonderregel vorliegt und
- es um Personenbezogene Daten geht und
- Datenverarbeitungsanlagen eingesetzt werden oder
- eine Verarbeitung in oder aus nichtautomatisierten Dateien stattfindet und
- keine ausschließlich persönlich oder familiäre Tätigkeiten vorliegen

☑ Abgrenzung des Bereichs persönlicher Lebensführung von beruflicher und geschäftlicher Sphäre.

☑ Äußerer Rahmen, organisatorische Anlage und inhaltliche Konzeption müssen persönliche/familiäre Zwecksetzung erkennen lassen.

☑ Beispiel: Nutzung einer Adressdatei auf PC von allen Familienmitgliedern.

☑ Bei intensiven Rechtseingriffen: Abwehransprüche aus BGB möglich.

## 2.1 ANWENDUNGSBEREICH

### § 2 BDSG – Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stelle gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

- sie über den Bereich eines Landes hinaus tätig werden oder
- Dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

## 2.2 DEFINITIONEN

§1 BDSG

[...]

(2) Dieses Gesetz gilt für die Erhebung,  
Verarbeitung und Nutzung personenbezogener  
Daten durch

[...]

Übergang Anwendungsbereich Definitionen -> (zunächst) nur noch BDSG  
Weisen die Daten keinen Personenbezug auf ist das BDSG schon nicht anwendbar

## 2.2 DEFINITIONEN

### Personenbezogene Daten

§ 3 Abs. 1 BDSG:

„[...] sind Einzelangaben über die persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“

Persönliche: Namen, Anschrift, Familiennamen, Geburtsdatum, Fingerabdrücke, Gesundheitszustand, Bankverbindung, Fotos, Beruf, persönliche Überzeugungen -> Identifikations, äußere, innere Zustände

Sachliche: Eigentumsverhältnisse, Informationen über Kommunikationsverhalten, vertragliche Beziehungen zu Dritten, Informationen zu Nutzungsverhalten Dritter ->

Bestimmbare = Informationen, die durch entsprechendes Zusatzwissen zugeordnet werden können, z.T. problematisch etwa bei Personen im Gruppenakkord oder Cookies, Relativität des Personenbezugs

Natürliche Personen nur lebende, keine juristischen Personen (hM)

## 2.2 DEFINITIONEN

Zwischenfragen:

Welche Informationen sind personenbezogene Daten:

- Name und Adresse einer Person
- Telefonnummer
- Matrikelnummer
- IP-Adresse
- Quellcode eines Computerprogramms

alle außer Quellcode, IP-Adresse fraglich aber hM sagt ja

## 2.2 DEFINITIONEN

A ist alleiniger Gesellschafter und Geschäftsführer einer GmbH. Unternehmen B speichert in einer Datenbank Angaben über den Umsatz, Gewinn und die Kreditwürdigkeit der A GmbH.

Sachlicher Anwendungsbereich ist eröffnet, da GmbH klein genug ist, dass Schlüsse auf die Person des A möglich sind.

## 2.2 DEFINITIONEN

### anonyme/pseudonyme Daten

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Anonymisiert: Entfernen identifizierender Merkmale, so dass eine Zuordnung nicht mehr bzw. nur noch mit unverhältnismäßigem Aufwand möglich ist

Pseudonomysierung: Zuordnung über bestimmte Regel möglich, Zusatzwissen notwendig (Bspe. Chat Nick, Kunden Nr., IP Adresse)

Es kommt auf das Verhältnis zum Aufwand an

Aggregierte sind auch anonym

## 2.2 DEFINITIONEN

### Erhebung

§ 3 Abs. 3 BDSG:

„Erheben ist das Beschaffen von Daten über den  
Betroffenen“

Legaldefinition dabei gilt der Grundsatz der Unmittelbarkeit § 4 Abs. 2 direkt beim Betroffenen, außer in den dort geregelten Ausnahmefällen (zielgerichtetes) Beschaffen von Daten des Betroffenen

### Verarbeitung

§ 3 Abs. 4 BDSG:

„Verarbeiten ist das Speichern, Ändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der angewendeten Verfahren:

- Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
- Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
- Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass
  - a) die Daten an den Dritten weitergegeben werden oder
  - b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruf,
- Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
- Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.“

Art. 2 lit b DSRL, alle Phasen und Maßnahmen der Verarbeitung vgl. next; technikneutral, weiter, da Erhebung und Nutzung in D diff.  
einzelne Schritte der Verarbeitung: Verändern führt zu einem neuen o. geänderten Informationsgehalt; Übermitteln: Weitergabe/Veröffentlichung, Bereithalten zum Abruf

## 2.2 DEFINITIONEN

### Nutzung

§ 3 Abs. 5 BDSG:

„Nutzen ist jeder Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.“

Klassischer Auffangtatbestand, relativ spät in das Gesetz aufgenommen

## 2.2 DEFINITIONEN

### verantwortliche Stelle

§ 3 Abs. 7 BDSG:

„... ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“

Wer auch immer die Daten für sich selbst oder im Auftrag (§ 11 BDSG) durch Dritte erhebt, verarbeitet oder nutzt „Herrin der Daten“, entscheidet über Zwecke und Mittel

Erheblich, wo die Stelle „Sitz“ hat, nicht wo sie tätig ist. Art 4 DSRL als Kollisionsregel

NB: Stelle ist immer jur. Person → kein Konzernprivileg, selbst, sobald unabhängig tätig

Div. Unternehmen ↔ Behörden; Einheits- ↔ Gliederungstheorie

2 lit d DSRL, 3 VII BDSG

## 2.2 DEFINITIONEN

### Besondere Arten personenbezogener Daten

§ 3 Abs. 9 BDSG:

„[...] sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.“

Besonders geschützt, Verarbeitung nur unter erhöhten Voraussetzungen, z.B. gesonderte Einwilligung notwendig  
Besonderes Gefahrenpotential

Sind folgende Angaben besondere personenbezogene Daten?

- Vorliegen einer Krebserkrankung
- Austritt aus der Kirche
- Teilnahme an einer Demonstration gegen Studiengebühren
- Passbild eines Brillenträgers
- Ausübung einer Risikosportart
- Mitgliedschaft in einem Schachclub

- Frau Geschwätzig berichtet dem Vermieter, dass ihr Nachbar schon im Gefängnis gesessen habe.
- Sachbearbeiter Fleißig notiert sich Informationen aus einem Telefonat auf einem Schmierzettel.
- Herr und Frau Ängstlich haben auf ihrem Grundstück eine Videoüberwachungsanlage installiert. Eine Kamera erfasst auch ein Stück des Garten des Nachbars.
- Die Baustoffhandel GmbH führt Papierpersonalakten.
- Der Betriebsrat druckt eine Liste aller Nicht-Gewerkschaftsmitglieder aus und gibt diese an die Gewerkschaft als Papierausdruck weiter.

**03  
ZULÄSSIGE  
DATENVERARBEITUNG  
NACH BDSG**

Im seltenen Fall, dass BDSG einschlägig ist (beschränkt auf Regelfall der privatwirtschaftlichen Datenverarbeitung)

### 3 BDSG

- Rechtmäßigkeit
- Zweckbindung
- Erforderlichkeit
- Transparenz
- Betroffenenrechte
- Datensicherheit
- Kontrolle

## Verbot mit Erlaubnisvorbehalt

§ 4 Abs. 1 BDSG

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“

Umgang mit personenbezogenen Daten nur dann zulässig, wenn dazu eine gesetzliche Regelung besteht oder eine Einwilligung des Betroffenen gegeben wurde.

**§ 4a Einwilligung**

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Nb freie Entscheidung nur wenn informiert und keine Zwangslage

Koppelungsverbot nur im TMG, die Leistung darf nicht abhängig sein von Angaben, die nicht zur Leistung notwendig sind

Weiteste gestattung (+/- alles mögl)

Diff öff r und priv Bereich, wenn gesetzl Grdlge gegeben, muss diese auch im priv Bereich genannt werden, sonst evtl Täuschg über Wirkg d Widerrufs

**Inhaltliche Voraussetzungen**

Art 2 lit. h DSRL, §

In Kenntnis der Sachlage (wer verarbeitet welche Daten zu welchem Zweck?)

! Kann bei asymmetrischen Verhältnissen zur Formalie verkommen → Koppelungsverbot im 12 III TMG und bei Marktbeherrschung Arbeitsverhältnis

Kommerzialisierung der Einwilligung (Abkaufen von Daten)

**Formale Voraussetzungen**

Str. ob Abgabe höchstpersönlich, Vertretg muss jedoch möglich sein

Form: 4a I 3 BDSG Schriftform 126, 126a BGB auch elektronisch, Ausnahme möglich eg 4a II

Elektronische Einwilligung im TMG ist anderes

Wenn zusammen mit anderen Erklärungen besonders hervorheben

## 3 BDSG - Rechtmäßigkeit

### § 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist,

a) zur Wahrung berechtigter Interessen eines Dritten oder

b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungsrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um länderübergreifende oder sonst zusammenfassende Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbeziehung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuzufügen. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 3a Satz 1 gespeichert wird, in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung für die Nutzung der Daten von der verantwortlichen Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4 Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit ablesen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Sät die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftlichen Schuldverhältnisses über die verantwortliche Stelle sowie über die Widerspruchsrechte nach Satz 1 zu unterrichten; soweit der Ansprache personenbezogener Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftlichen Schuldverhältnisses.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlicher Stellen nur unter den Voraussetzungen des § 14 Abs. 2 zulässig. Die Übermittelnde Stelle hat hierauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4 Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung

**§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke**

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

5/6

Datenverarbeitung ist Hilfsmittel für die Erfüllung bestimmter geschäftlicher, beruflicher oder gewerblicher Zwecke

z.B. DV dient dazu die im Rahmen eines Vertrags anfallenden Daten zur Verfügung zu stellen, nb Arbeitnehmer nun gesondert geregelt

Nr. 1 Vertrag als Grundlage, alles was für die Abwicklung nach gemeinsamen Vertragswillen notwendig ist

Nr. 2 und Abs. 2 Interessenabwägung als Grundlage: Erforderlichkeit; Interessenabwägung: berechnigte Interessen des Datenverarbeiters gegen schutzwürdige Interessen des Betroffenen

Sonderfälle

### 3 BDSG - Rechtmäßigkeit

Sonderfälle der Datenverarbeitung zu eigenen Zwecken:

- Besondere Arten personenbezogener Daten, §§ 4a, 28 Abs. 6 ff.
- Datenverarbeitung zu Werbezwecken, § 28 Abs. 3
- Datenübermittlung an Auskunftfeien, § 28a
- Datenverwendung im Rahmen von Scoring, § 28b
- Datenverarbeitung im Rahmen eines Beschäftigungsverhältnisses, § 32

### 3 BDSG - Rechtmäßigkeit

Datenverarbeitung für fremde Zwecke  
§§ 29 ff. BDSG

Datenverarbeitung wird zum Selbstzweck  
Daten werden zur Ware, die Ziel und Gegenstand der DV bestimmt  
zB Auskunftfeien, Adresshändler

**§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung**

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunftsteilen oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder
3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Absatz 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

(6) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

gilt grds. für Adresshändler Auskunftsteile etc..

Sonderfälle: § 28 Abs. 3 für Adresshändler,

28b Scoring,

30, 30a: Gewerbsmäßige Datenverwendung für Zwecke der Markt- und Meinungsforschung

### 3 BDSG - Rechtmäßigkeit

Andere Rechtsvorschriften:

- Auskunftsverlangen nach AO
- Vereinssatzung
- Betriebsvereinbarung
- Tarifvertrag

cave: Schutzniveau des BDSG darf nicht unterlaufen werden

### 3 BDSG - Zweckbindung

Zweckbindung und Zweckänderung

Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden,

### 3 BDSG - Zweckbindung

Zweckbindung und Zweckänderung?

Adressdaten werden für die Zusendung bestellter Ware erhoben und danach zum Versand des neuen Kataloges verwendet.

Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden,

Zulässig, wenn dies rechtmäßig, erforderlich, transparent ist und die Anforderungen an die Datensicherheit sowie die Rechte der Betroffenen eingehalten werden.

Also: § 4 Absatz 1 entweder Einwilligung oder Rechtsgrundlage.

### 3 BDSG - Erforderlichkeit

#### Erforderlichkeit

- Einzelfallbetrachtung
- Datensparsamkeit
- Löschung

Die Datenverarbeitung ist nach Art, Umfang, Intensität auf den für den Zweck der Datenverarbeitung notwendigen Umfang zu begrenzen.

Einzelfallbetrachtung: Datenerhebung muss für Zweckerfüllung unverzichtbar sein

-Keine Datenerhebung auf Vorrat

- Datensparsamkeit: § 3b Bundesdatenschutzgesetz - Gestaltung von Verarbeitungssystemen
- Löschung § 35 Abs. 2 Nr. 3 BDSG - Zweckerfüllung / Aufbewahrungsfristen - Sperrung

### 3 BDSG - Transparenz

- Direkterhebung, § 4 Abs. 2
- Unterrichtungspflicht, § 4 Abs. 3
- Benachrichtigungspflicht, § 33
- Besondere Informationspflichten, §§ 6a Abs. 2 Nr. 2, 6b Abs. 2, 6c Abs. 1

Personenbezogene Daten sind beim Betroffenen zu erheben

4 III: Info über Identität der verantwortlichen Stelle, Zweckbestimmungen, Kategorien der Empfänger

33: Nachträgliche Info bei Speicherung ohne Kenntnis

6a: Automatisierte Einzelfallentscheidung 6b: Videoüberwachung 6c: Chipkarte

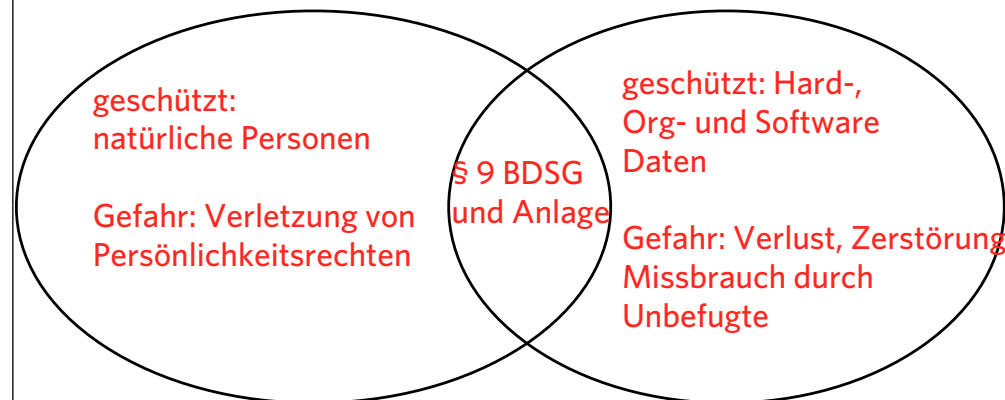
### 3 BDSG - Betroffenenrechte

- Auskunft, § 34 Abs. 1-4
- Berichtigung, § 35 Abs. 1
- Löschung, § 35 Abs. 2
- Sperrung, § 35 Abs. 3 und 4
- Widerspruch, § 35 Abs. 5

**Auskunft:-** Sämtliche zum Kunden gespeicherten Daten- Herkunft der Daten - Empfänger, an die Daten weitergegeben werden - Zweck der Speicherung

**Löschung:** zB wenn nicht mehr benötigt

**Sperrung:** zB wenn nicht mehr benötigt, Aufbewahrung aber vorgeschrieben



Datenschutz: Schutz der Menschen vor Missbrauch, Kontrolle des Einzelnen über seine Daten


Datensicherheit: Grundlage des Datenschutzes, Schutz der Daten und ihrer Verarbeitung vor unberechtigten Zugriffen/Zerstörung

#### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. 

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Abstrakte Formulierung von Anforderungen an technische und organisatorische Maßnahmen  
Als Maßstab für Infrastruktur und Grundlage für Schutzmaßnahmen erzeugen Kontrollfähigkeit und Testbarkeit

#### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. [§ 9](#)

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.


Zutrittskontrolle: zB Chipkartensysteme, biometrische Maßnahmen, Besuchermanagement, Schlüssel, Zäune etc...

#### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. 

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.


# Zugangskontrolle: Kennwortgeschützte System, Entsorgungsprozess, Firewalls

### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. 

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

# Zugriffskontrolle: Berechtigungssystem (logische) Verschluss (physische)

### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. **FD**

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.


# Weitergabekontrolle: Verschlüsselung, Protokollierung

### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. 

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.


# Eingabekontrolle: Protokollierung, zeitlich und personell gebundene Zugriffsrechte

#### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. 

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

## Auftragskontrolle: Verträge, Vorortkontrollen/Audits

### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. **FS**

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.


# Verfügbarkeitskontrolle: Redundanz, Backups, Wartung, Patch- und Updatemanagement

#### § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

#### Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten **getrennt** verarbeitet werden können. 

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

# Datentrennung: keine abteilungsübergreifende Datennutzung, rollenbasierte Zugriffsberechtigung

### 3 BDSG - Datensicherheit

#### Technische Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Zurechenbarkeit
- Nichtabstreitbarkeit

#### Datenschutz Schutzziele:

- Intervenierbarkeit
- Transparenz
- Unverkettbarkeit

**Vertraulichkeit:** Informationen dürfen nur dem Berechtigten bekannt werden (wer darf welche Daten lesen?)

**Integrität:** Informationen sind richtig und vollständig oder dies ist erkennbar nicht der Fall (wer darf welche Daten ändern?)

**Verfügbarkeit:** Informationen sind zugänglich, wann und wo sie vom Berechtigten benötigt werden

**Authentizität (Überprüfbarkeit der Echtheit und Glaubwürdigkeit) und Zurechenbarkeit** lassen sich mit digitalen Signaturen erreichen

### 3 BDSG - Datensicherheit

#### Technische Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Zurechenbarkeit
- Nichtabstreitbarkeit

#### Datenschutz Schutzziele:

- Intervenierbarkeit
- Transparenz
- Unverkettbarkeit

**Intervenierbarkeit:** das System muss dem Betroffenen die Ausübung seiner Rechte gewährleisten

**Transparenz:** Ist ein Maß für die Beobachtbarkeit von korrekten, relevanten, verständlichen und umfassenden Informationen, mit dem Ziel eine breite und solide Grundlage für Entscheidungsprozesse zu schaffen, oder auf Basis dieser Informationen bereits getroffene Entscheidungen zu legitimieren. **Nicht Verkettbarkeit:** ist die fehlende Möglichkeit der Zuordnung

- mehrerer Kommunikationsvorgänge (bzw. der daraus resultierenden Daten) zueinander,
- bestimmter Kommunikationsvorgänge (bzw. der daraus resultierenden Daten) zu bestimmten Individuen oder
- verschiedener Individuen zueinander.

**§ 4f Beauftragter für den Datenschutz**

(1) Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für die nichtöffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

789

Bestellungspflicht: unabhängig von der Anz d MA: Satz 6 DV zum Zwecke der Übermittlung, Anonymisierung, Markt und Meinungsforschung DV, die Vorabkontrolle (§4d V) verlangt.

Abhängig v Anz MA: S 1–4, ab zehn MA, die ständig mit der Verarbeitung personenbezogener Daten betraut sind, ab 20 Bestellung intern oder extern, schriftlich

**§ 4f Beauftragter für den Datenschutz**

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

Stellung im Unternehmen: Geschäftsleitung direkt unterstellt, in Ausübung seiner Fachkunde weisungsfrei, Benachteiligungsverbot und Kündigungsschutz, Unterstützung durch Leitung, Beendigung durch Fristablauf, einvernehmliche Beendigung, Amtsniederlag, Wiederruf nur in wichtigen Fällen (§626 BGB)

#### § 4g Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen

Hinwirken auf die Einhaltung des DSR, Überwachung der ordnungsgemäßen Einhaltung der DVProgramme, Schulungen der MA, Ansprechpartner für DS Fragen, Führen des Verfahrensverzeichnis, Durchführung von Vorabkontrollen

04

Vertiefung und  
Wiederholung - 1

Im seltenen Fall, dass BDSG einschlägig ist (beschränkt auf Regelfall der privatwirtschaftlichen Datenverarbeitung)

#### 4 Vertiefung und Wiederholung

Unter welchen Umständen ist eine Datenverarbeitung nach dem Bundesdatenschutzgesetz zulässig?

81

- Rechtmäßigkeit
- Zweckbindung
- Erforderlichkeit
- Transparenz
- Betroffenenrechte
- Datensicherheit
- Kontrolle

#### 4 Vertiefung und Wiederholung

Was besagt das datenschutzrechtliche „Verbot mit Erlaubnisvorbehalt“?

#### 4 Vertiefung und Wiederholung

Nennen Sie drei Voraussetzungen einer wirksamen Einwilligung nach § 4a BDSG.

freie Entscheidung, Widerrufbarkeit, Schriftlichkeit, Informationspflicht, Bestimmtheit, str. höchstpersönliche Abgabe, gesonderter Hinweis,

4 Vertiefung und Wiederholung

Wodurch wird der datenschutzrechtliche Grundsatz der  
Transparenz sichergestellt?

Direkterhebungsgrundsatz, § 4 Abs. 2 BDSG,  
Informationspflicht, §§ 4 Abs. 3, 4a Abs. 1 S. 2 BDSG  
Unterrichtungspflicht, eg §§ 16 Abs. 3, 19a Abs. 1, 33 Abs. 1 BDSG  
Auskunftsanspruch, § 34 BDSG

4 Vertiefung und Wiederholung

Erläutern Sie das datenschutzrechtliche Prinzip der Kontrolle!

85

extern: Kontrollbehörde

intern: DSB (Fachkunde und Zuverlässigkeit, Sensibilisierung)

Verfahrensverzeichnis: §§ 4g II, 4e S. 1

#### 4 Vertiefung und Wiederholung

Wo ist die Datenverarbeitung durch nichtöffentliche Stellen im BDSG geregelt?

Dritter Abschnitt, §§ 27–32 BDSG

#### 4 Vertiefung und Wiederholung

Wodurch unterscheidet sich die Datenverarbeitung für eigene Zwecke (§ 28 BDSG) von der für fremde Geschäftszwecke (§§ 29, 30 BDSG)??

87

eigene Zwecke: Datenverarbeitung (DV) ist Hilfsmittel für die Erfüllung eigener geschäftlicher, beruflicher oder gewerblicher Zwecke; Verarbeitung dient dazu, die im Rahmen von Verbraucherverträgen wie bspw. Kaufverträgen anfallenden Daten für den spezifischen Vertragszweck zur Verfügung zu stellen.

fremde Zwecke: DV wird zum Selbstzweck; Daten werden zur Ware, die Ziel und Gegenstand der Verarbeitung ist.

#### 4 Vertiefung und Wiederholung

Nennen Sie den Hauptanwendungsfall der Datenverarbeitung für eigene Geschäftszwecke!

88

§ 28 Abs. 1 Nr. 1 BDSG; DV zur Vertragserfüllung ist zulässig, wenn ein sachlicher Zusammenhang zu dem Vertrag besteht und diese erforderlich ist.

Erforderlichkeit ≠ Dienlichkeit, = kein milderes, weniger einschneidendes Mittel steht zur Erfüllung des selben Zwecks zur Verfügung

#### 4 Vertiefung und Wiederholung

Welche Interessen sind bei der Datenverarbeitung nach § 28 Abs. 1 Nr. 2 BDSG abzuwägen?

89

DV erforderlich für die Wahrung berechtigter (rechtlicher, wirtschaftlicher, ideeller) Interesse, das nicht durch eine objektiv zumutbare Alternative gewahrt werden kann.  
gegen schutzwürdige Interessen des Betroffenen (Art der Daten, Intensität der Verarbeitung, Widerspruch des Betroffenen)

Exkurs 28 I Nr. 3: allgemein zugängliche Daten, Hintergrund: Grundrecht auf Informationsfreiheit (Art. 5 I GG), sehr enge Ausnahme: schutzwürdige Interessen des Betroffenen überwiegen offensichtlich, Bspe für allgemein zugängliche Quellen.

#### 4 Vertiefung und Wiederholung

Nennen Sie die Voraussetzungen für eine Zweckänderung bei der Datenverarbeitung für eigene Zwecke!

90

§ 28 Abs. 2 BDSG, keine schutzwürdigen Interessen stehen entgegen und

- Voraussetzungen I Nr. 2 oder 3 sind erfüllt (Nr. 1)
- Erforderlichkeit zur Wahrung berechtigter Interessen eines Dritten (Nr. 2a)
- Erforderlichkeit zur Gefahrenabwehr oder Strafverfolgung (Nr. 2b)

Erforderlichkeit für Durchführung wissenschaftlicher Forschung, besondere Interessenabwägung (Nr. 3)

Exkurs Behördenanfragen: hier nur Auskunftsrecht keine Pflicht, diese nur aus Spezialgesetz (zB StPO)

4 Vertiefung und Wiederholung

Erläutern Sie das so genannte Listenprivileg!

91

Ausnahme zur 28 III 1 (Einwilligungserfordernis) in S. 2: DV ist erforderlich zu einem der in Nrn. 1-3 genannten Gründe (Werbung für eigene Angebote, beim Betroffenen oder aus allgemein zugänglichen Quellen erhoben; im Hinblick auf berufliche Tätigkeit; für Spenden); keine schutzwürdigen Interessen stehen entgegen. **Von Listenprivilegerfasste Daten:**  Zugehörigkeit zu einer Personengruppe  Berufs-, Branchen- oder Geschäftsbezeichnung  Name  Titel  Akademischer Grad  Anschrift  Geburtsjahr

#### 4 Vertiefung und Wiederholung

##### § 28 Abs. 3a (elektronische Einwilligung)

Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

92

- Protokollierung
- Erklärung jederzeit abrufbar
- Erklärung jederzeit widerrufbar

#### 4 Vertiefung und Wiederholung

##### § 28 Abs. 4 (Widerspruchsrecht)

Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses. 93

## Widerspruchsrecht gegen Verarbeitung und Nutzung von Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung

- Widerspruchshinweis \_ Bei Vertragsschluss \_ Im Rahmen der Werbung

#### 4 Vertiefung und Wiederholung

### § 28 Abs. 6-9 (besondere Arten personenbezogener Daten, § 3 Abs. 9 BDSG)

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 2 Nummer 2 Buchstabe b gilt entsprechend.

- Z.B.: Gesundheitsdaten, Mitgliederdaten von Kirchen, Gewerkschaften, Parteien
- Durchsetzung rechtlicher Ansprüche, § 28 VIII BDSG, Interessenabwägung! Vergleich: Bei einfachen Daten genügt es, wenn DV dem Vertrag dient.
- Verarbeitungsbefugnisse für Ärzte und medizinisches Personal, d.h. Beschränkung auf Schweigepflichtige, § 28 VII BDSG
- Strafverfolgung: erhebliche Gefahren, erhebliche Straftaten, § 28 VIII BDSG  
Vergleich: nach II Nr. 2b) genügt jede Straftat

#### 4 Vertiefung und Wiederholung

##### § 29 Abs. 1 (DV zum Zwecke der Übermittlung)

Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,
  2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder
  3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.
- § 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

95

- Erheben, Speichern, Verändern, Nutzen pbD ▪ Insbesondere für Zwecke der Werbung, Auskunfteitätigkeit, Adresshandel
- Nr. 1: Keine schutzwürdigen Interessen an dem Ausschluss der DV
- Nr. 2: Daten aus allgemein zugänglichen Quellen, es sei denn, schutzwürdige Interessen stehen entgegen
- Nr. 3: Voraussetzungen des § 28a I oder II BDSG erfüllt

## 4 Vertiefung und Wiederholung

### § 28a Datenübermittlung an Auskunfteien

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4. a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten. 96

- Zweck: Transparenz und Schaffung eindeutiger Rechtsgrundlagen
- Absatz 1: Befugnis zum Einmelden von Schuldnerdaten (Negativdaten) ist nunmehr abschließend geregelt
- Wichtigste Fallgruppen:
  - ┌ Fälligkeit einer Forderung, 2 Mahnungen, zeitlicher Abstand,
  - Androhung der Einmeldung, Forderung nicht bestritten
  - ┌ Forderung ist ausdrücklich anerkannt
  - ┌ Forderung durch rechtskräftiges Urteil festgestellt
- Absatz 2
  - ┌ Kreditinstitute dürfen Informationen bspw. über Darlehen und Kontoeröffnungen einmelden (sog. „Positivinformationen“)
  - ┌ Keine offensichtlich überwiegenden schutzwürdigen Interessen der Betroffenen
  - ┌ Unterrichtung des Betroffenen
  - ┌ Keine Übermittlung von Konditionenanfragen

#### 4 Vertiefung und Wiederholung

##### § 28b Scoring

Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,
2. im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunft die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,
3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,
4. im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

97

- Gesetzlich normierte Voraussetzungen für die Durchführung von Scoring:
  - ┌ Wahrscheinlichkeitswerte müssen auf einem wissenschaftlichen Verfahren beruhen
  - ┌ Genutzte Daten müssen für Berechnung der Wahrscheinlichkeit eines bestimmten Verhaltens erheblich sein
  - ┌ Keine ausschließliche Nutzung von Anschriftendaten
  - ┌ Über Nutzung von Anschriftendaten (neben anderen Daten) muss unterrichtet werden
- Spezielle Auskunftsrechte in § 34 Abs. 2 und Abs. 4 BDSG