Dr. Harald Vinke

Medienrecht II

4. Teil
Datenschutzrecht

Gliederung

A. Einführung

Datenschutzrecht = **Querschnittsmaterie**

d.h. datenschutzrechtliche Aspekte finden sich in jedem Rechtsgebiet

➔ auch im Internet- und Medienrecht

Das Datenschutzrecht dient dem **Persönlichkeitsschutz** vor Technik und Informationsinfrastrukturen.

Für die Gefahren der neuen Informationstechnologie reichten in den 70er Jahren die herkömmlichen Instrumente (Gegendarstellung, Unterlassungsanspruch) nicht mehr aus.

Folge: Verlagerung des Schutzes auf das Vorfeld von Persönlichkeitsrechtsverletzungen

I. Geschichte

70er Jahre: Erkenntnis, dass durch bloße Datenverarbeitung das Persönlichkeitsrecht beeinträchtigt werden kann.

1977 erstes BDSG

1983 Volkszählungsurteil des BVerfG (BVerfGE 65, S. 1 ff.)

Ausgehend von der Erkenntnis, dass der Einzelne sich unter Beobachtung seiner Umwelt anders – und nicht frei – verhält, wurde (staatliche) Informationsverarbeitung unter einen Gesetzesvorbehalt gestellt.

Diese Konzeption wurde auch auf den privaten („nicht-öffentlichen“) Bereich übertragen.

Folge: umfangreiche Datenschutzregelungen in vielen Gesetzen.

➔ bereichsspezifischer Datenschutz

90er Jahre: das Internet führt zu strukturell neuen Problemen

1997: Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG)

sollte einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste schaffen

Artikelgesetz:

Inhalt:

1. drei neue Gesetze

- *TeledienstegG*
- *Gesetz über den Datenschutz bei Telediensten (TDDG)*

} Nachfolger: **TMG** (2007)

- Gesetz zur digitalen Signatur

2. Änderungen bestehender Gesetze: z.B. Strafgesetzbuch.

Rechtssetzung auf europäischer Ebene

1995: Richtlinie 95/46/EG (Datenschutz**richtlinie**)

Mindeststandards für den Datenschutz, die in allen Mitgliedstaaten der EU durch nationale Gesetze sichergestellt werden

2002: Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)

24.05.2016: Datenschutz-Grundverordnung tritt in Kraft

Exkurs: Rechtsakte der EU	
Richtlinie	**Verordnung**
Den einzelnen **Mitgliedstaatenbleibt** überlassen, wie sie die Richtlinien umsetzen. Sie haben bei der Umsetzung der Richtlinie ei-	EU-Rechtsakte, die allgemeine Geltung haben, in allen ihren Teilen verbindlich sind und **unmittelbar** in jedem Mitgliedstaat gelten. Sie müssen von den EU-Mitgliedstaaten nicht in nationales

nen gewissen **Spielraum**. Nach deutschem Recht ist zur Umsetzung in der Regel ein förmliches Gesetz oder eine Verordnung erforderlich. Richtlinien setzen regelmäßig eine Frist, innerhalb derer sie in innerstaatliches Recht umgesetzt werden müssen. Wird eine Richtlinie nicht fristgerecht oder nicht ordnungsgemäß umgesetzt, kann sie dennoch unmittelbar wirken und von Behörden angewendet werden. Dazu muss die Richtlinienbestimmung inhaltlich so genau und konkret gefasst sein, dass sie sich zu einer unmittelbaren eignet und sie darf keine unmittelbare Verpflichtung für einen Einzelnen beinhalten.	Recht umgesetzt werden. Modifikationen der vorgegebenen Regelungen durch die einzelnen Mitgliedstaaten sind grundsätzlich nicht möglich.

Datenschutz-Grundverordnung gilt ohne Umsetzungsakt unmittelbar in allen EU-Mitgliedstaaten, allerdings erst ab dem 25. Mai 2018.

Den Mitgliedstaaten ist es grundsätzlich nicht erlaubt, den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken.

Allerdings enthält die Verordnung verschiedene Öffnungsklauseln, die es den einzelnen Mitgliedstaaten ermöglichen, bestimmte Aspekte des Datenschutzes auch im nationalen Alleingang zu regeln.

= "Hybrid" zwischen Richtlinie und Verordnung

Inhalt:

1. Ein Kontinent, ein Recht:

Die Verordnung wird eine einheitliche Datenschutzregelung schaffen, die EU-weit gültig ist. Unternehmen müssen damit nur noch ein Gesetz anstelle von 28 befolgen.

2. Das Recht auf Vergessenwerden wird gestärkt:

Wenn Bürger keine weitere Verarbeitung ihrer Daten wünschen und kein legitimer Grund für die Speicherung der Daten vorliegt, muss der Verantwortliche die Daten löschen, es sei denn er kann nachweisen, dass sie weiterhin erforderlich oder relevant sind. Außerdem werden die Bürger im Fall eines Hacker-Angriffs besser informiert. Das Recht auf Datenübertragbarkeit wird es Benutzern erleichtern, personenbezogene Daten zwischen Diensteanbietern zu übertragen.

3. Europäische Regeln auf europäischem Boden:

Unternehmen mit Sitz außerhalb Europas werden dieselben Regeln befolgen müssen, wenn sie Dienstleistungen in der EU anbieten.

4. Erweiterte Befugnisse für unabhängige nationale Datenschutzbehörden:

Die Behörden werden gestärkt, damit sie die Regeln wirksam durchsetzen können. Sie werden befugt, Geldbußen über Unternehmen zu verhängen, die gegen die EU-Datenschutzbestimmungen verstoßen. Dies kann Strafzahlungen von bis zu 1 Mio. Euro bzw. 2% des Jahresumsatzes des Unternehmens nach sich ziehen.

5. Zentrale Anlaufstellen:

Die Regeln sehen zentrale Anlaufstellen für Unternehmen und Bürger vor. Unternehmen müssen sich nur noch an eine einzige Aufsichtsbehörde statt an 28 richten, wodurch es für sie einfacher und günstiger wird, EU-weit Geschäfte zu tätigen. Einzelpersonen können sich an die nationale Datenschutzbehörde ihres Landes in ihrer eigenen Sprache wenden, selbst wenn ihre personenbezogenen Daten außerhalb dieses Landes verarbeitet werden.

II. Datenschutzgesetze

1. Bund

- Bundesdatenschutzgesetz (BDSG)
- Für den **Internet- und Telekommunikationsbereich**: TMG, RStV und TKG
- StPO
- G-10
- BVerfSchG

2. Länder

- Landesdatenschutzgesetze
- Polizeigesetze

B. Begriffe des Bundesdatenschutzgesetzes

I. Adressat des Datenschutzrechts

"**verantwortliche Stelle**“ (früher „speichernde Stelle“).

= die jeweilige Behörde (vgl. § 1 Abs. 4 VwVfG) bzw. Person des Privatrechts, die Daten verarbeitet.

auch der Auftragsdatenverarbeiter

Ausgenommen vom Anwendungsbereich des Datenschutzrechts ist die rein private und familiäre Datenverarbeitung.

II. Geschützter

der von der Datenverarbeitung „**Betroffene**“.

= natürliche Person

Datenschutzrecht erfasst nur „**personenbezogene Daten**“

= Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren **natürlichen Person** (§ 3 Abs. 1 BDSG)

Es kommt nicht darauf an, wie schutzbedürftig und sensibel das einzelne Datum ist.

Nicht erfasst sind anonyme Daten und Sachdaten.

III. Erhebung, Verarbeitung und Nutzung von Daten

1. Erhebung

= Beschaffen von Daten über den Betroffene

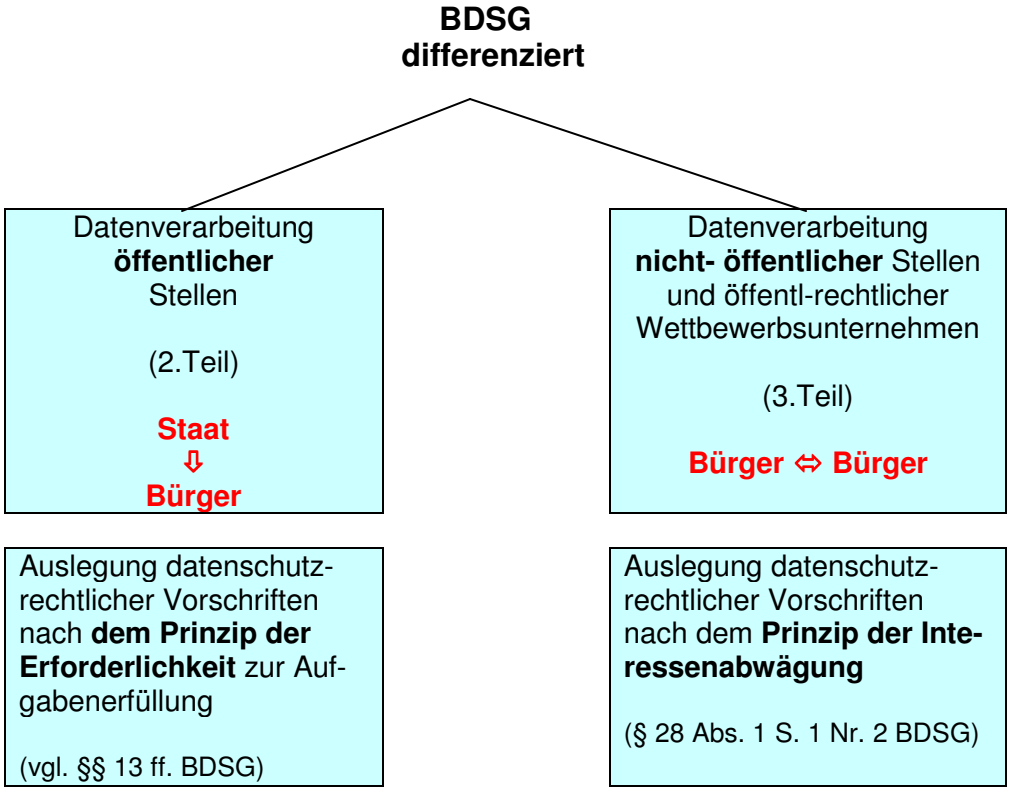
Es bedarf einer Aktivität, durch die die erhebende Stelle oder Person Kenntnis von den Daten erhält oder Verfügung über diese begründet.

2. Verarbeitung von Daten

- Speicherung
- Veränderung
- Übermittlung
- Sperrung
- Löschung

C. Prinzipien des Datenschutzrechts

Ausgangspunkt: „**Verbot mit Erlaubnisvorbehalt**“.



Für beide Bereiche gelten folgende Grundsätze:

I. Datenvermeidung und Datensparsamkeit (§ 3a BDSG)

§ 3a BDSG - Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Es sollen nur die personenbezogenen Daten verarbeitet werden, die für ein konkretes Vorhaben erforderlich sind.

Dabei ist nicht quantitativ auf die Menge der Daten abzustellen, sondern **qualitativ** auf den Grad des Personenbezugs.

Verfahren, die einen Personenbezug vermeiden, sind vorzuziehen.

II. Eingeschränkte Zulässigkeit der Datenerhebung

- wenn durch Gesetz erlaubt
- bei Einwilligung des Betroffenen

§ 4 BDSG - Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
(1) 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.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2.
a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

III. Transparenz

Volkszählungsurteil des BVerfG:

⇨ „**Informationelle Selbstbestimmung“**

= der Einzelne muss einen Überblick über seine informationelle Umwelt haben.

Mittel:

- Unterrichtung (§ 4 Abs. 3 BDSG)
- Benachrichtigung (§§ 19a, 33 BDSG)
- Auskunft (§§ 19, 34 BDSG)
- weitere Informations- und Meldepflichten (§§ 4d ff. BDSG).

1. Informationspflichten

- Der Datenverarbeiter muss die Datenverarbeitungsverfahren der Aufsichtsbehörde (§ 4d Abs. 1 BDSG) oder dem betrieblichen bzw. behördlichen Beauftragten für den Datenschutz melden (§ 4g Abs. 2 S. 1 BDSG).
- Der Öffentlichkeit („Jedermann“) ist auf Nachfrage eine Verfahrensübersicht (§ 4e BDSG) zur Verfügung zu stellen.
- Für bestimmte Branchen (Detekteien, Auskunfteien) bestehen darüber hinaus besondere behördliche Meldepflichten (§ 4d Abs. 4 BDSG, § 38 GewO).
- Der Betroffene ist bei Erhebung über die Umstände der Datenverarbeitung zu unterrichten.

  Information über die Identität des Verarbeiters (und ggf. von Dritten, an die Daten weitergegeben werden) und den Zweck der Verarbeitung.

  Hinweis auf besonders persönlichkeitsrechtsgefährdende Verarbeitungsarten (z.B. Profilerstellung, automatische Einzelentscheidung, Cookies)

  Im **Internetbereich** muss darüber hinaus über die Verarbeitung der Daten außerhalb der EU bzw. des EWR informiert werden (➔TMG).

  Weitere Unterrichtungspflichten können sich aus dem Fernabsatzrecht ergeben.

- Hinweis auf Freiwilligkeit, wenn die Preisgabe von Daten nicht auf einer Rechtsvorschrift beruht (§ 4 Abs. 3 S. 2 BDSG).

  Wenn im **Internet** eine anonyme bzw. pseudonyme Nutzung möglich ist, muss der Nutzer auch darüber unterrichtet werden (§ 13 Abs. 6 S. 2 TMG).

- Soweit spezielle Widerspruchsrechte bestehen, sind diese dem Betroffenen mitzuteilen (§ 28 Abs. 4 S. 2 BDSG). Dies gilt auch für die Widerrufbarkeit der Einwilligung sowie für die Folgen deren Verweigerung (§ 13 Abs. 3 TMG).

- Wenn die Daten nicht beim Betroffenen erhoben worden sind, ist er hierüber grundsätzlich zu benachrichtigen (§§ 19a, 33 BDSG).

2. Auskunftsrecht

- Recht des Betroffenen auf Auskunft (§§ 19, **34 BDSG**), das teilweise über die Benachrichtigungspflicht hinausgeht.

  Die Auskunft hat unentgeltlich und regelmäßig schriftlich zu erfolgen.

  Ausnahmen zum Schutz von Amts- und Geschäftsgeheimnissen

  Das Auskunftsrecht ist nicht abdingbar (§ 6 BDSG).

BDSG

Zweiter Abschnitt
Datenverarbeitung der öffentlichen Stellen

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.
(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.
(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.
(7) Die Auskunft ist unentgeltlich.

Dritter Abschnitt
Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 34 Auskunft an den Betroffenen

(1) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über
1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.
(1a) Im Fall des § 28 Absatz 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über
1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,
2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und

3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle
1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder
2. bei einer anderen Stelle gespeicherte Daten nutzt.

Hat eine andere als die für die Entscheidung verantwortliche Stelle
1. den Wahrscheinlichkeitswert oder
2. einen Bestandteil des Wahrscheinlichkeitswerts
berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. Im Fall des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie die Auskunft nicht selbst erteilt. In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. Die Pflicht der für die Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,
2. die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,
2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,
3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie
4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle
1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder
2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(7) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(8) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder
2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten zu verschaffen. Er ist hierauf hinzuweisen.

BGH, Urt. v. 28.01.2014 – VI ZR 156/13 (Scorewerte der SCHUFA)

Die Klägerin machte gegen die Bekl. einen datenschutzrechtlichen Auskunftsanspruch geltend.

Die Wirtschaftsauskunftei Schufa sammelt und speichert im Rahmen ihrer Tätigkeit personenbezogene Daten, die für die Beurteilung der Kreditwürdigkeit der Betroffenen relevant sein können. Darüber hinaus erstellt sie, u. a. auch unter Berücksichtigung der hinsichtlich des jeweiligen Betroffenen vorliegenden Daten, sogenannte Scorewerte. Ein Score stellt einen Wahrscheinlichkeitswert über das künftige Verhalten von Personengruppen dar, der auf der Grundlage statistisch-mathematischer Analyseverfahren berechnet wird. Die von der Bekl. ermittelten Scores sollen aussagen, mit welcher Wahrscheinlichkeit der Betroffene seine Verbindlichkeiten vertragsgemäß erfüllen wird.

Ihren Vertragspartnern stellt die Bekl. diese Scorewerte zur Verfügung, um ihnen die Beurteilung der Bonität ihrer Kunden zu ermöglichen.

Im Oktober 2011 scheiterte zunächst die Finanzierung eines Automobilkaufs der Kl. aufgrund einer falschen Negativauskunft der Bekl. Die Kl. wandte sich daraufhin telefonisch an die Bekl. und forderte die Zusendung einer Bonitätsauskunft an, die die Bekl. mit Schreiben vom 28. 10. 2011 erteilte. Die Auskunft beinhaltete die bei der Bekl. gespeicherten persönlichen Daten der Kl. sowie die Mitteilung, dass der Bekl. im Übrigen keine Informationen vorlägen.

Nachdem die Kl. die Bekl. aufgefordert hatte, zu der zunächst erteilten falschen Negativauskunft Stellung zu nehmen, übersandte diese der Kl. mit Schreiben vom 22. 12. 2011 eine „Datenübersicht“ nach § 34 BDSG. Neben den gespeicherten persönlichen Daten der Kl. und allgemeinen Informationen zur Bekl. sowie zum Scoringverfahren enthielt diese die Auflistung von Anfragen Dritter und die in Bezug auf die Kl. im November und Dezember 2011 übermittelten sowie ihre aktuellen Wahrscheinlichkeitswerte. Die aktuellen Wahrscheinlichkeitswerte waren nach verschiedenen branchenbezogenen Scores getrennt; bei den übermittelten Wahrscheinlichkeitswerten wurde der zugehörige Branchenscore ebenfalls angegeben. Die Darstellung aller Wahrscheinlichkeitswerte erfolgte dabei mit dem jeweiligen Scorewert, der Ratingstufe, der prozentualen Erfüllungswahrscheinlichkeit, der Auflistung verschiedener Datenarten sowie der Bedeutung insgesamt. Bei den Datenarten wurde jeweils dargestellt, ob sie verwendet oder nicht verwendet wurden. Im Fall der Verwendung erfolgte die Einordnung in eine von fünf näher bezeichneten Risikostufen. Die Gesamtbedeutung wurde ebenfalls in verschiedenen Risikokategorien verbalisiert.

Nach Klageerhebung im Februar 2012 übersandte die Bekl. der Kl. am 20. 4. 2012 eine neue „Datenübersicht“ nach § 34 BDSG, die der vorangegangenen Übersicht insbesondere in der Darstellung der Wahrscheinlichkeitswerte entsprach.

Die Kl. war der Ansicht, die von der Bekl. erteilte Auskunft genüge nicht den gesetzlichen Anforderungen, sie sei insbesondere nicht transparent. Für die Kl. sei nicht hinreichend nachvollzieh-

bar, wie einzelne Branchen-Scorewerte zustande gekommen seien. Diese stünden in Widerspruch zur hervorragenden Bonität der Kl. Die Bekl. sei insbesondere verpflichtet, die einzelnen Elemente, die in die Berechnung der Scores eingeflossen seien, offenzulegen. Sie müsse Angaben zu den Vergleichsgruppen machen, in die sie die Kl. zur Berechnung der Scores eingeordnet habe.

Das AG hat die Bekl. zur Rückzahlung der von der Kl. für die Bonitätsauskunft gezahlten Vergütung verurteilt und die auf Auskunftserteilung, Zahlung vorgerichtlicher Anwaltskosten sowie Korrektur der Scorewerte gerichtete Klage im Übrigen abgewiesen.

Die dagegen eingelegte Berufung der Kl. und die Anschlussberufung der Bekl. hatten keinen Erfolg.

Die Revision der Kl., mit der sie lediglich die Ansprüche auf Auskunft und auf Zahlung weiterverfolgte, hatte keinen Erfolg.

BDSG § 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 Auskunftei 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.

IV. Die Einwilligung

§ 4a BDSG – 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.

Grundform: Schriftform (§ 4a Abs. 1 S. 3 BDSG)

- mit den vorgeschriebenen Unterrichtungen verbunden
- Wird sie zusammen mit anderen rechtlichen Erklärungen abgegeben (z.B. durch AGB), ist sie besonders hervorzuheben.

  Für die Erklärung der Einwilligung im Internet gelten Erleichterungen bezüglich der Form (§ 13 Abs. 2 TMG).

daneben: generelles Widerspruchsrecht (§ 20 Abs. 5, § 35 Abs. 5 BDSG) sowie ein spezielles Widerspruchsrecht gegen die Nutzung der Daten für Werbezwecke (§ 28 Abs. 4 S. 2 BDSG).

D. Datenschutzkontrolle

I. Rechte der Betroffenen

Voraussetzung für Kontrolle: Kenntnis des Betroffenen von der Datenverarbeitung.

wird gewährleistet:

➔ durch die Informationspflichten des Verarbeiters

➔ durch nicht abdingbaren Auskunftsanspruch gegen den Verarbeiter im Einzelfall

Auf der Grundlage der Kenntnis der ihn betreffenden Datenverarbeitung kann der Betroffene

- Berichtigung
- Löschung,
- Sperrung
- und/oder Gegendarstellung

seiner Daten verlangen, wenn diese falsch sind oder unrechtmäßig gespeichert werden.

Wenn der Betroffene durch die Datenverarbeitung einen (materiellen oder immateriellen) Schaden erleidet, hat er Anspruch auf Schadenersatz.

➔ § 823 Abs. 2 BGB i. V. mit einer als Schutzgesetz zu qualifizierenden Norm des BDSG

➔ § 7 BDSG und (nur für öffentliche Stellen) aus § 8 BDSG

§§ 43, 44 BDSG Bußgeld und Strafbarkeit

II. Interne Selbstkontrolle

Überwachung der Datenverarbeitung liegt nicht primär nicht in den Händen staatlicher Behörden, sondern wird innerhalb der verantwortlichen Stelle erbracht.

➔ durch betriebliche oder behördliche Beauftragte für den Datenschutz

Der Beauftragte für den Datenschutz ist unabhängig, aber gegenüber dem Verarbeiter nicht weisungsbefugt.

III. Datenschutzbehörden

keine zentrale Aufsichtsbehörde für den Datenschutz

➔ föderale Struktur

Zuständig

- für die Bundesverwaltung und für die Überwachung des Telekommunikationsdatenschutzes

  ➔ Bundesdatenschutzbeauftragter

- für Überwachung des übrigen nicht-öffentlichen Sektors sowie der Landesverwaltung (einschließlich der Auftragsverwaltung)

  ➔ Länder

  hier unterschiedliche Organisationsmodelle:

  z.T. Aufsicht über öffentliche und nicht-öffentliche Datenverarbeitung beim Landesdatenschutzbeauftragten zusammengeführt

  z.T. Trennung dieser beiden Bereiche

  ➔ Kontrolle der Wirtschaft durch die Innenbehörden

  ➔ Kontrolle der Verwaltung durch den Landesdatenschutzbeauftragten.

IV. Wettbewerber/Verbraucherschutzverbände

wettbewerbsrechtlicher Unterlassungsanspruch (§ 8 UWG) bei Datenschutzverstößen

E. Internationaler Datenschutz

I. (Räumlicher) Anwendungsbereich

Es gilt das **Sitzprinzip**, d.h.:

Für alle verantwortlichen Stellen mit Sitz in Deutschland sowie für die hiesigen Niederlassungen ausländischer Stellen gilt deutsches Datenschutzrecht.

Hat der Verarbeiter seinen Sitz in einem Staat der EU bzw. des EWR, gilt für ihn bei Verarbeitungen in Deutschland das Recht seines Sitzlandes, allerdings durchgesetzt von den deutschen Aufsichtsbehörden.

Umgekehrt unterliegen Verarbeiter mit Sitz in Deutschland bei Verarbeitungen in der EU nur deutschem Recht.

Hat der Verarbeiter seinen Sitz in einem Staat außerhalb der EU/EWR, gilt für seine Verarbeitungen in Deutschland deutsches Recht.

Problem: "Verarbeitung in Deutschland"

II. Datenexport

innerhalb der EU: grenzenloser Datenverkehr

EU- Datenschutzrichtlinie verbietet grundsätzlich, personenbezogene Daten aus EG-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EG-Recht vergleichbares Datenschutzniveau verfügen.

Dies sind im Wesentlichen nur die EWR-Staaten (EU, Norwegen, Island, Liechtenstein), die Schweiz und (teilweise) die USA **("safe harbor-Vereinbarung"**) und Kanada.

Für alle anderen Staaten:

die verantwortliche Stelle hat selbst das Datenschutzniveau zu beurteilen.

➔ einzelfallbezogen
➔ alle Umstände (technische und juristische) sind zu berücksichtigen.

Wenn kein „angemessenes Schutzniveau“ festgestellt oder hergestellt werden kann, ist die Übermittlung in den Drittstaat nur in bestimmten Fällen möglich

- Einwilligung
- zur Erfüllung eines Vertrages mit oder zugunsten des Betroffenen
- bei Gefahr für Leib und Leben
- im Rahmen von Gerichtsverfahren (einschließlich Vorverfahren)

- aus öffentlichen Registern
- zum Schutz der öffentlichen Sicherheit und Ordnung.

Aktuell:

EuGH, Urt. v. 06.10.2015 – C-362/14 (Maximilian Schrems v. Data Protection Commissioner – "Safe Harbour")

Der Europäische Gerichtshof (EuGH) hat entschieden, dass die Safe Harbor Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG) („Safe Harbor Entscheidung") ungültig ist, da die USA kein angemessenes Datenschutzniveau gewährleistet.

Hintergrund:

Wenn personenbezogene Daten ins Ausland übermittelt werden, stellt sich die Frage, nach welcher gesetzlichen Grundlage dies datenschutzrechtlich erlaubt ist (§§ 4b, 4c BDSG).

- Innerhalb der EU bzw. des Europäischen Wirtschaftsraums ist die Übermittlung relativ problemlos möglich

  ➔ Es gibt ein harmonisiertes europäisches Datenschutzrecht.

- Problem: Daten sollen in Staaten *außerhalb des Europäischen Wirtschaftsraums* übermittelt werden

  Artikel 25 Abs. 1 der Datenschutzrichtlinie 95/46/EG:

  Datenübermittlung in „Drittstaaten" ist nur erlaubt, **wenn dort ein *angemessenes Schutzniveau* gewährleistet** ist.

  Safe Harbor-Entscheidung der **Kommission** (Entscheidung 2000/520/EG) vom 26.07. 2000 stellte **für die USA** ein solches Schutzniveau fest – mit Bindungswirkung auch für die Datenschutzbehörden der Mitgliedsstaaten.

  ➔ Datenfluss in die USA legitimiert

- jetzt:

  EuGH stützt seine Entscheidung auf eine Prüfung der Safe Harbor-Entscheidung der Kommission selbst.

  EuGH hat keine *eigene* Bewertung des Datenschutzniveaus in den USA vorgenommen, sondern lediglich geprüft, ob die Entscheidung der Kommission die seiner Ansicht nach relevanten Punkte überhaupt *berücksichtigt* hat.

  EuGH sieht Fehler, die zu einer Ungültigkeit der Safe Harbor-Entscheidung führen:

- Safe Harbor-Entscheidung hat in die Unabhängigkeit der nationalen Datenschutzbehörden eingegriffen. Diese müssen in völliger Unabhängigkeit prüfen können, ob eine Entscheidung der Kommission den Anforderungen der Datenschutzrichtlinie entspricht

- Ein angemessenes Schutzniveau ist nicht vorhanden, wenn die Safe Harbor-Grundsätze lediglich für eine Selbstzertifizierung von US-*Unternehmen* gelten, jedoch nicht für amerikanische Behörden. Das Recht des Drittstaats selbst muss den Schutz *gewährleisten* und effektive Schutzmechanismen enthalten.

- Es ist nicht mit dem Wesensgehalt des Grundrechts auf Achtung des Privatlebens vereinbar, wenn amerikanische Behörden ohne jegliche Differenzierung, Einschränkung oder Ausnahme Zugriff auf die Daten der Betroffenen haben.

- Die Kommission hätte sicherstellen müssen, dass betroffenen Personen bei Eingriffen in ihre Grundrechte ein effektiver Rechtsschutz zur Verfügung steht, um ihre datenschutzbezogenen Rechte durchzusetzen (z.B. Berichtigung oder Löschung).

Konsequenzen:

Eine Übermittlung personenbezogener Daten ist (grundsätzlich) auch ohne eine Safe Harbor-Zertifizierung möglich. Sie unterliegt nach dem Urteil des EuGH aber gegebenenfalls höheren Anforderungen.

Folgende Alternativen sind denkbar:

1. Gesetzliche Ausnahmen (Art. 26 Abs. 1 DSRL):

Ausnahmsweise kann die Übermittlung personenbezogener Daten zulässig sein, sofern eine der Ausnahmen nach Art. 26 (1) (a)-(f) DSRL zutrifft:

- Wenn die Übermittlung personenbezogener Daten zum Beispiel zum Abschluss oder zur Erfüllung eines Vertrages notwendig ist.
- Wenn die betroffene Person (z.B. ein Facebook-Nutzer) der Datenübermittlung zustimmt. Eine wirksame Einwilligung muss allerdings bestimmten formellen Vorschriften entsprechen (z.B. § 4aBDSG, § 13 Abs. 2 TMG).

2. EU Standardvertragsklauseln:

Gemäß Art. 26 Abs. 4 DSRL hat die Kommission Standardvertragsklauseln entwickelt, die ein angemessenes Datenschutzniveau sicherstellen. Nach dem Urteil des EuGH wird nun diskutiert, ob die Standardvertragsklauseln noch ein angemessenes Datenschutzniveau gewährleisten.

3. Binding Corporate Rules (BCR):

BCRs sind verbindliche Richtlinien, die Unternehmen bei sich implementieren können, um für konzerninterne Übermittlungen personenbezogener Daten in unsichere Drittstaaten das erforderliche Datenschutzniveau sicherzustellen.

Aber noch offen, ob sie nach dem EuGH Urteil noch ein wirksames Instrument für die Datenübermittlung in die USA darstellen.

4. Wie geht es weiter?

Die EU-Kommission hat in einer offiziellen Stellungnahme festgestellt, dass ihrer Auffassung nach die Standardvertragsklauseln und BCRs weiterhin als Instrument für die internationale Übermittlung genutzt werden können.

Einige nationale Datenschutzbehörden bezweifeln die Wirksamkeit der Standardvertragsklauseln. (Dass sie hierzu die Möglichkeit haben, hat der EuGH ja betont.)

Wenn Standardvertragsklauseln und BCRs als Optionen für die Datenübermittlung in die USA wegfallen, hätte dies weitreichende Auswirkungen, insbesondere für Unternehmen, deren Geschäftsmodell von einer Datenübermittlung in die USA abhängig ist, z.B. Cloud-Provider.

Der Bezug des EuGH auf die Grundrechtscharta wird Auswirkungen auf verschiedene zukünftige Rechtsbestimmungen haben, die gerade verhandelt werden.

F. Datenschutz in bestimmten Bereichen

I. Öffentliche Stellen/Verwaltung

Die Datenverarbeitung **durch öffentliche Stellen** ist im zweiten Teil des BDSG (§§ 12 ff. BDSG) und in den Landesdatenschutzgesetzen geregelt.

BDSG: Datenverarbeitung durch **Bundesbehörden**

§ 12 BDSG - Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder
2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.
(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Absatz 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16 und 19 bis 20.

§ 13 BDSG - Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.
(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,
3. 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,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
7. 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,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder
9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14 BDSG - Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. 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 Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es 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) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder
2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche 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.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 15 BDSG - Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 10 Abs. 4 bleibt unberührt.

(3) Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 16 BDSG - Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn
1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 17

(weggefallen)

§ 18 BDSG - Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

1. Anwendungsbereich

alle personenbezogenen Datenverarbeitungen durch die öffentliche Hand

aber teilw. bereichsspezifische Regelungen

- Datenverarbeitung im Rahmen der Strafverfolgung ist in der **StPO** geregelt
- Datenverarbeitung im Rahmen der allgemeinen Gefahrenabwehr ist in den **Polizeigesetzen** geregelt

2. Verarbeitungsgrundsätze

Volkszählungsurteil: personenbezogene Datenverarbeitungen müssen wie Grundrechtseingriffe behandelt werden

Folge: es gelten in Bezug auf die Datenverarbeitung die allgemeinen verwaltungsverfahrensrechtlichen Prinzipien

➔ Gesetzesvorbehalt/Prinzip des geringstmöglichen Eingriffs

Zulässigkeit: orientiert sich grundsätzlich an der Aufgabenstellung der jeweiligen Behörde

wenn die Datenverarbeitung zur „Erfüllung der Aufgabe […] erforderlich" ist (vgl. §§ 13 Abs. 1, 14 Abs. 1 S. 1 BDSG)

➔ Erforderlichkeit bemisst sich nach der Aufgabe, die außerhalb des BDSG festgelegt ist.

Grundsatz der Zweckbindung: personenbezogene Daten dürfen nur innerhalb der Zweckbestimmung, der ihrer Erhebung zugrunde lag, verarbeitet werden.

Zweckänderungen sind nur in den gesetzlich vorgesehenen Fällen (z.B. § 14 Abs. 2 BDSG) zulässig.

Beschränkung auf Behörde ("Stelle"):

Datenschutzrecht stellt nicht auf den Staat als juristische Person ab, sondern auf die Behörde im funktionellen Sinne.

Folge: Datenaustausch innerhalb eines Landes oder des Bundes oder einer Gemeinde ist deshalb nicht ohne weiteres möglich.

Datenaustausch muss sich an dem Maßstab für die „Übermittlung“ messen lassen (§ 15 BDSG).

II. Datenverarbeitung nicht-öffentlicher Stellen

§ 28 BDSG - 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.

(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 Forschungseinrichtung 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 listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, 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 hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a 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 die für die Nutzung der Daten verantwortliche 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 § 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.

(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 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.

(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 nichtöffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf 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 § 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 Strafgesetzbuchs 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 regelmäßig 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.

1. Vertragsverhältnisse

Für eigene Geschäftszwecke sind Datenverarbeitungen nach der (gemeinsamen) Zweckbestimmung des Vertragsverhältnisses grundsätzlich (und ohne Abwägung von Interessen) gestattet (§ 28 Abs. 1 S. 1 Nr. 1 BDSG).

➔ Belange des Betroffenen werden durch die Freiwilligkeit des Vertragsschlusses gewahrt.

Für Verarbeitungen, die von der Zweckbestimmung des Vertrages nicht gedeckt werden (etwa Überprüfung der Kreditwürdigkeit), oder wenn kein Vertrag besteht, muss der Verarbeiter seine „berechtigten Interessen“ gegen die „schutzwürdigen Interessen“ des Betroffenen abwägen (§ 28 Abs. 1 S. 1 Nr. 2 BDSG).

Wenn weder der Vertragszweck noch eine Interessenabwägung die Datenverarbeitung gestatten, kann nur noch auf die Einwilligungserklärung der Betroffenen zurückgegriffen werden.

z.B. **SCHUFA-Klausel**

Problem: **Direktwerbung**

Datenschutzrechtlich ist Direktwerbung grundsätzlich erlaubt (siehe § 28 Abs. 4 S. 2 BDSG), denn Verstopfung von Briefkästen ist keine Persönlichkeitsrechtsgefährdung durch Informationstechnik.

Datenschutzrechtlich relevant ist der vorgelagerte Bereich

➔ **Adresshandel** und Adressselektion.

Verkauf und Vermietung von Kundendaten sind nicht verboten, aber Einwilligung erforderlich (vgl. § 28 Abs. 3 BDSG)

Grenze für Direktwerbung: § 7 UWG

2. Datenschutz im Medienbereich

Problem:

Spannungsverhältnis

Pressefreiheit (Art. 5 Abs. 1 S. 1 GG)	⇔	Persönlichkeitsrecht des Betroffenen auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG)

a) Anwendbare Normen

"Medienrecht" ist in verschiedenen Gesetzen geregelt

Regelungen für Datenschutz dementsprechend **aufgeteilt**:

- PresseG
- RStV
- Gesetze/Staatsverträge über öffent-rechtl. Rundfunkanstalten
- § 41 Abs. 2ff BDSG für Deutsche Welle.

§ 41 BDSG - Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien
(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

b) Medienprivileg

Gesetzgeber verzichtet hier auf das „Verbot mit Erlaubnisvorbehalt“.

Es gibt nur die "Rahmenvorschrift" des § 41 Abs. 1 BDSG

➔ Bereich des Mediendatenschutzes wird weitgehend der Selbstregulierung und den allgemeinen Vorschriften überlassen.

➔ Pressekodex

G. Datenschutz im Internet

§ 11 TMG - Anbieter-Nutzer-Verhältnis

(1) Die Vorschriften dieses Abschnitts gelten nicht für die Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien, soweit die Bereitstellung solcher Dienste

1. im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder
2. innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

(2) Nutzer im Sinne dieses Abschnitts ist jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

(3) Bei Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, gelten für die Erhebung und Verwendung personenbezogener Daten der Nutzer nur § 15 Absatz 8 und § 16 Absatz 2 Nummer 4.

§ 12 TMG - Grundsätze

(1) Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(3) Soweit nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht automatisiert verarbeitet werden.

§ 13 TMG - Pflichten des Diensteanbieters

(1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

(2) Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

(3) Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Absatz 2 Nr. 4 hinzuweisen. Absatz 1 Satz 3 gilt entsprechend.

(4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden,
3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
5. Daten nach § 15 Abs. 2 nur für Abrechnungszwecke zusammengeführt werden können und
6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

An die Stelle der Löschung nach Satz 1 Nr. 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

(5) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(6) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

(7) Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

§ 14 TMG - Bestandsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten).

(2) Auf Anordnung der zuständigen Stellen darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

§ 15 TMG - Nutzungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

(2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.

(3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.

(5) Der Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden. § 14 Abs. 2 findet entsprechende Anwendung.

(6) Die Abrechnung über die Inanspruchnahme von Telemedien darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Telemedien nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.

(7) Der Diensteanbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung speichern. Werden gegen die Entgeltforderung innerhalb dieser Frist Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen, dürfen die Abrechnungsdaten weiter gespeichert werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist.

(8) Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur verwenden, soweit dies für Zwecke der Rechtsverfolgung erforderlich ist. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

§ 15a TMG - Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten
Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

I. Abgrenzung zwischen BDSG und Telemediengesetz

TMG ist das speziellere Gesetz

TMG regelt den Schutz personenbezogener Daten bei der Nutzung von Telemediendiensten i.S.v. § 1 Abs. 1 TMG.

II. Kernaussagen

Wie im allgemeinen Datenschutzrecht

- Erhebung und Verarbeitung personenbezogener Daten ist im Online-Bereich nur zulässig, soweit sie gesetzlich gestattet ist oder der Betroffene einwilligt (§ 12 Abs. 1 TMG).
- Voraussetzungen für eine wirksame elektronische Einwilligung: § 13 Abs. 2 TMG
- Der Betroffene ist über Art, Umfang, Ort und Zweck der Erhebung und Nutzung seiner Daten vor deren Erhebung zu informieren. Auch hat der Nutzer das Recht, die zu seiner Person gespeicherten Daten unentgeltlich – auch auf elektronischem Wege und auch bei kurzfristiger Speicherung der Daten – einzusehen (§ 13 Abs. 7 TMG).
- Die Erstellung von Nutzungsprofilen ist nur bei der Verwendung von Pseudonymen zulässig (§ 15 Abs. 3 TMG).
- Bestands- und Nutzungsdaten werden unterschieden und getrennt voneinander geregelt (§§ 14, 15 TMG)
- Dem Diensteanbieter ist es gestattet, Abrechnungsdaten auch für die Aufklärung der missbräuchlichen Inanspruchnahme seiner Dienste zu nutzen, wenn ihm tatsächliche Anhaltspunkte für einen entsprechenden Missbrauchsfall vorliegen (§ 15 Abs. 8 TMG). Es besteht eine Dokumentationspflicht.

LG Stuttgart, Urt. v. 01.11.2008 – 8 O 357/07, NJW 2008, 2048 (Sexversteigerung)

- Personenbezogene Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen, sofern es sich nicht um Abrechnungsdaten i.S.v. § 15 Abs. 4 TMG handelt.

Problem: Speicherung von IP-Adressen

LG Darmstadt, Urt. v. 25.01.2006 – 25 S 118/05
OLG Frankfurt a. M., Urt. v. 16.06.2010 – 13 U 105/07

III. Sonderproblem Web-Cookies

Im Mai 2011 lief die Frist zur Umsetzung der so genannten "Cookie Richtlinie" (RL 2009/136/EG) ab.

Die "Cookie-Richtlinie" hat zu einer Änderung in Art.5 III der Datenschutzrichtlinie für die elektronische Kommunikation (2002/58/EG) geführt, die zwingend in deutsches Recht umzusetzen ist.

Vorschlag zur **Änderung des TMG…**

Mögliche Ergänzung in § 13 TMG
…..

(8) Die Speicherung von Daten im Endgerät des Nutzers und der Zugriff auf Daten, die im Endgerät des Nutzers gespeichert sind, sind nur zulässig, wenn der Nutzer darüber entsprechend Absatz 1 unterrichtet worden ist und er hierin eingewilligt hat. Dies gilt nicht, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten elektronischen Informations- oder Kommunikationsdienst zur Verfügung stellen zu können.

….wurde abgelehnt

Aktuelle Rechtslage ist strittig.

2015: Bundeswirtschaftsministerium und Europäische Kommission halten Richtlinie für umgesetzt – ohne nähere Begründung!

Folgen für die Praxis?

Verwirrung!

1. Risikovariante: Weiter wie bisher und nur ein Hinweis auf Cookies in der Datenschutzerklärung auf Cookies.

2. Sichere Variante: Vor dem Setzen der Cookies wird eine Einwilligung eingeholt.

3. Mittelweg: Bei jedem Besuch prominenter Hinweis auf Cookies.