Auszug aus dem Fernkurs - betrieblicher Datenschutzbeauftragter gemäß § 4f Abs. 2 S. 1 BDSG

Referent:
Wirtschaftsinformatiker Michael J. Schüssler
Geprüfter und anerkannter EDV Sachverständiger,
zertifizierter externer Datenschutzbeauftragter gemäß § 4f BDSG,
ISO/IEC 27001 Foundation ISMS zertifiziert.

Präambel

Aus unserer langjährigen Erfahrung heraus resultierend wissen wir sehr wohl, dass dieser Fernkurs oder das Präsenztraining unseren Teilnehmern einiges abverlangt, jedoch sollte eine fundierte Datenschutzausbildung auf soliden Beinen stehen.

Den Ersten Schritt haben Sie bereits getan! Beim Rest begleiten wir Sie.

Wir stehen Ihnen nach Terminabsprache gerne mit Rat und Tat zur Verfügung.

Ihr EDV Sachverständigen- und Datenschutzbüro
Michael J. Schüssler
Wirtschaftsinformatiker, EDV Sachverständiger &
externer Datenschutzbeauftragter gemäß § 4f BDSG.

ANSCHRIFT
Hanauer Straße 71
63741 Aschaffenburg

Tel.: 06021 / 439 18 45
Mobil: 0179 / 49 48 941

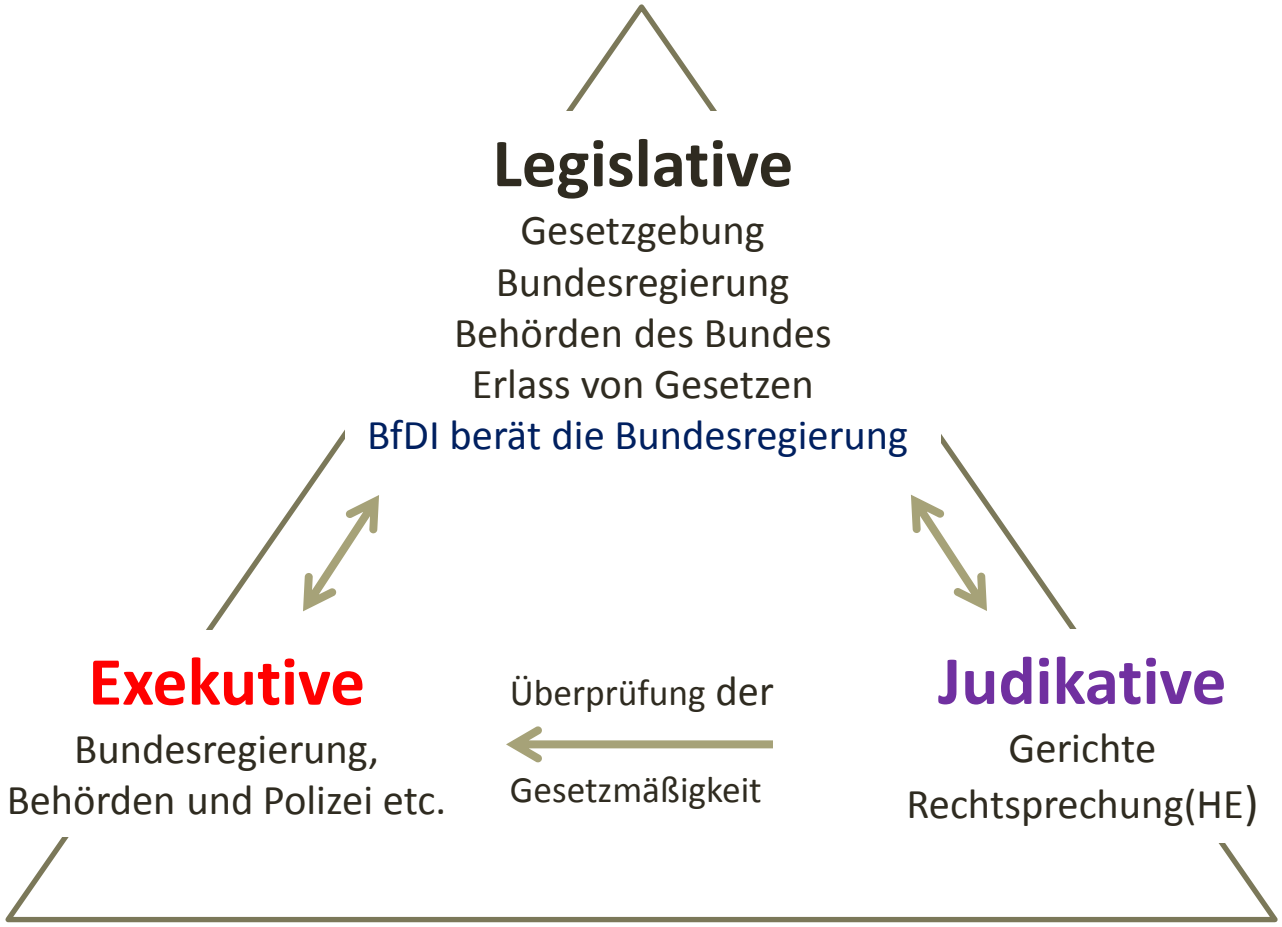
E-Mail: info@svb-ms.de
Internet: www.datenschutz4you.com
Internet: www.svb-ms.de

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

Die Gedanken sind frei. Wer kann sie erraten?

Datenschutz betrifft uns alle!

Gewaltenteilung in der Bundesrepublik Deutschland und die Stellung des BfDI



Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist der Beauftragte des Bundes sowohl für den Datenschutz als auch für die Informationsfreiheit - BSI Bundesamt für Sicherheit in der Informationstechnik.
Darüber hinaus gibt es die Datenschutzbeauftragten der Länder, insgesamt 16 Stück.

Zweck des Bundesdatenschutzgesetzes § 1 Abs. 1

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

Es wird das Persönlichkeitsrecht des Einzelnen geschützt, nicht die personen-bezogenen Daten oder die Person oder die Identität!

§ 2 Öffentliche und nicht-öffentliche Stellen

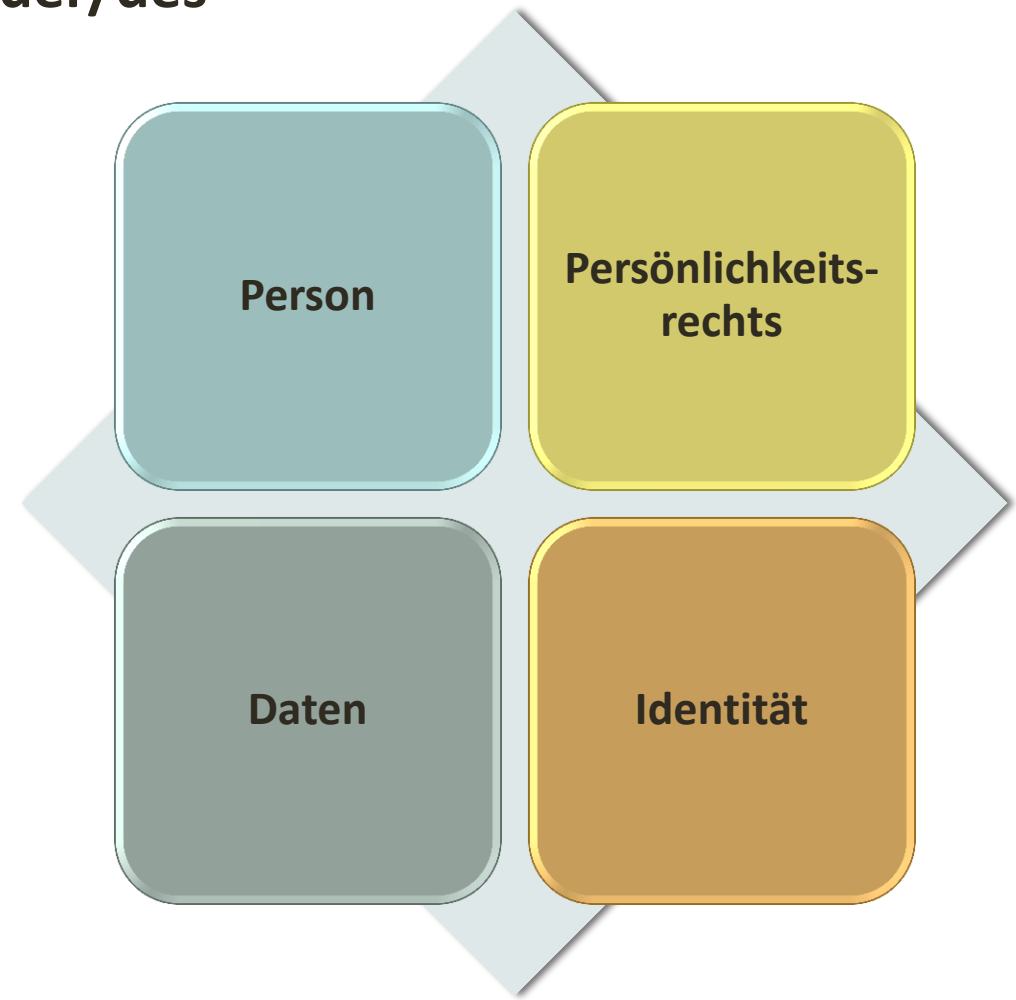
1. Öffentliche Stellen des Bundes sind die Behörden …
2. Öffentliche Stellen der Länder sind die Behörden …
3. Vereinigungen des privaten Rechts …, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes…

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 der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

Zusammenfassend - wen schützt das BDSG?

3

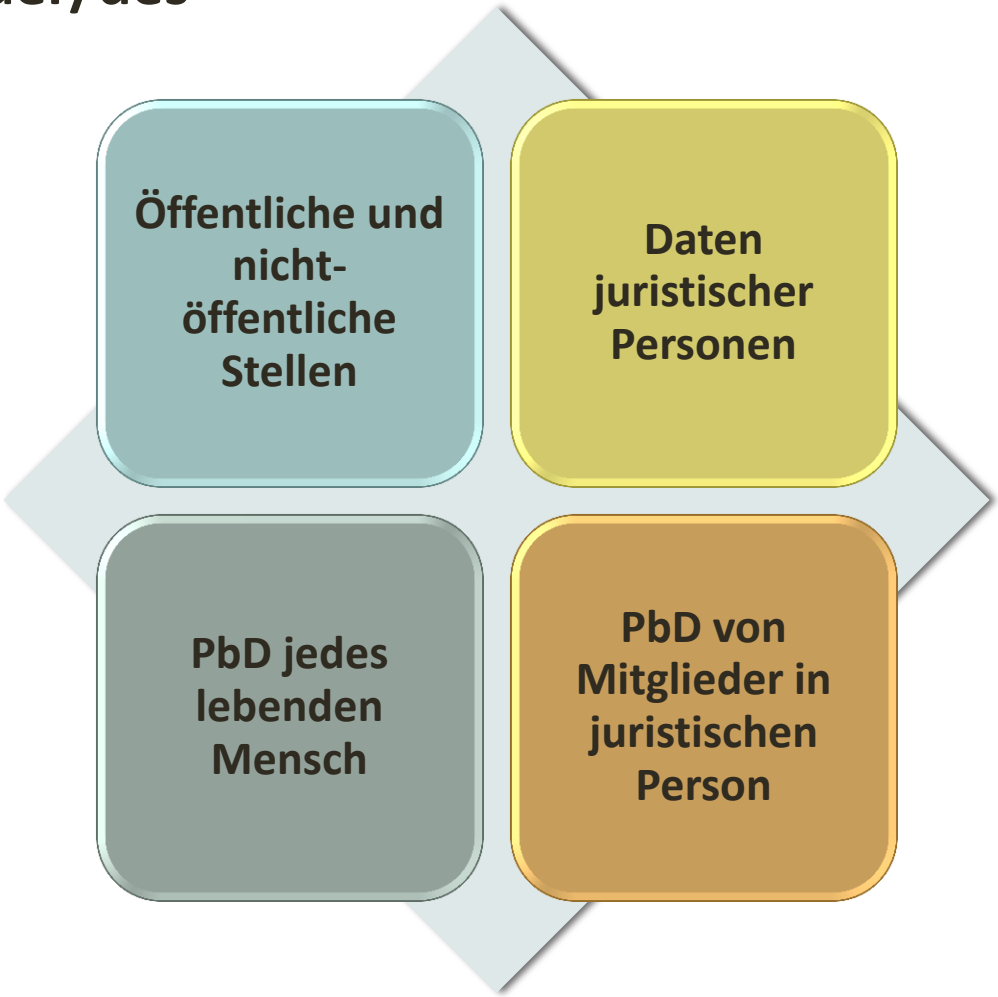
Schutz der/des



Kreuzen Sie bitte die richtige Lösung an.

Zusammenfassend - wen oder was schützt das BDSG?

Schutz der/des



Kreuzen Sie bitte die richtige Lösung an.

Personenbezogene Daten gemäß § 3 Abs. 1

1

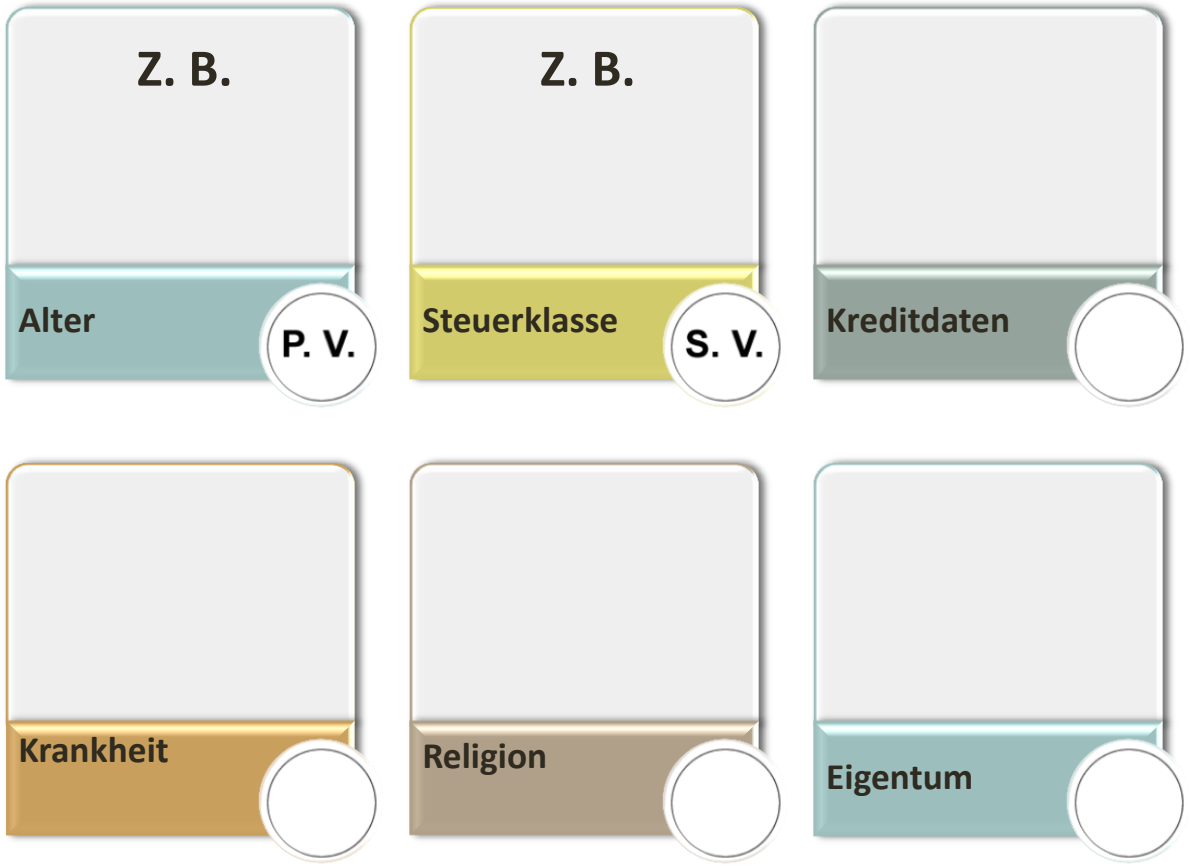
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Hans, Mustermann **Name** persönliche Verhältnisse	**Blau** **Augenfarbe** persönliche Verhältnisse	**183 cm** **Körpergröße** persönliche Verhältnisse
3.500 € brutto **Einkommen** sachliche Verhältnisse	**120.000 €** **Vermögen** sachliche Verhältnisse	**4711** **Steuernr.** sachliche Verhältnisse

Übungsaufgabe

2

Ordnen Sie die personenbezogene Daten den persönlichen oder sachlichen Verhältnissen zu.



Übung Arten von personenbezogenen Daten

2

1	Herr Schmitt fährt einen roten Porsche, Baujahr 2008.
2	Bei der letzten Bundestagswahl hat Frau Schön, die SPD gewählt.
3	Herr Klein ist bei der Gewerkschaft Verdi.
4	Name, Vorname, Anschrift einer Person.
5	Die Telefonnummer von Frau Karin Groß

1 = Bestimmte personenbezogene Daten

2 = Bestimmbare personenbezogene Daten

3 = Besonders sensible Daten

Übungsaufgabe - Schutzstufen A bis E

Ordnen Sie den nachfolgend genannten Prozessen oder Datenkategorien, Schutzstufen von (A bis E) zu und begründen Sie Ihre Einstufung.

Stufe A: B: C: D: E: **Begründung** 1

Meldepfl. Infektionskrankheiten

Stufe A: B: C: D: E: **Begründung** 2

Schufa Auskunft

Stufe A: B: C: D: E: **Begründung** 3

Adressdaten

Lösungsbeispiel

Stufe A:✓ B: C: D: E: **Begründung** 4

Geburtsjahr einer Person — Frei zugänglich - Listenprivileg

Stufe A: B: C: D: E: **Begründung** 5

Zeuge einer strafbaren Handlung

Datenschutzpanne:

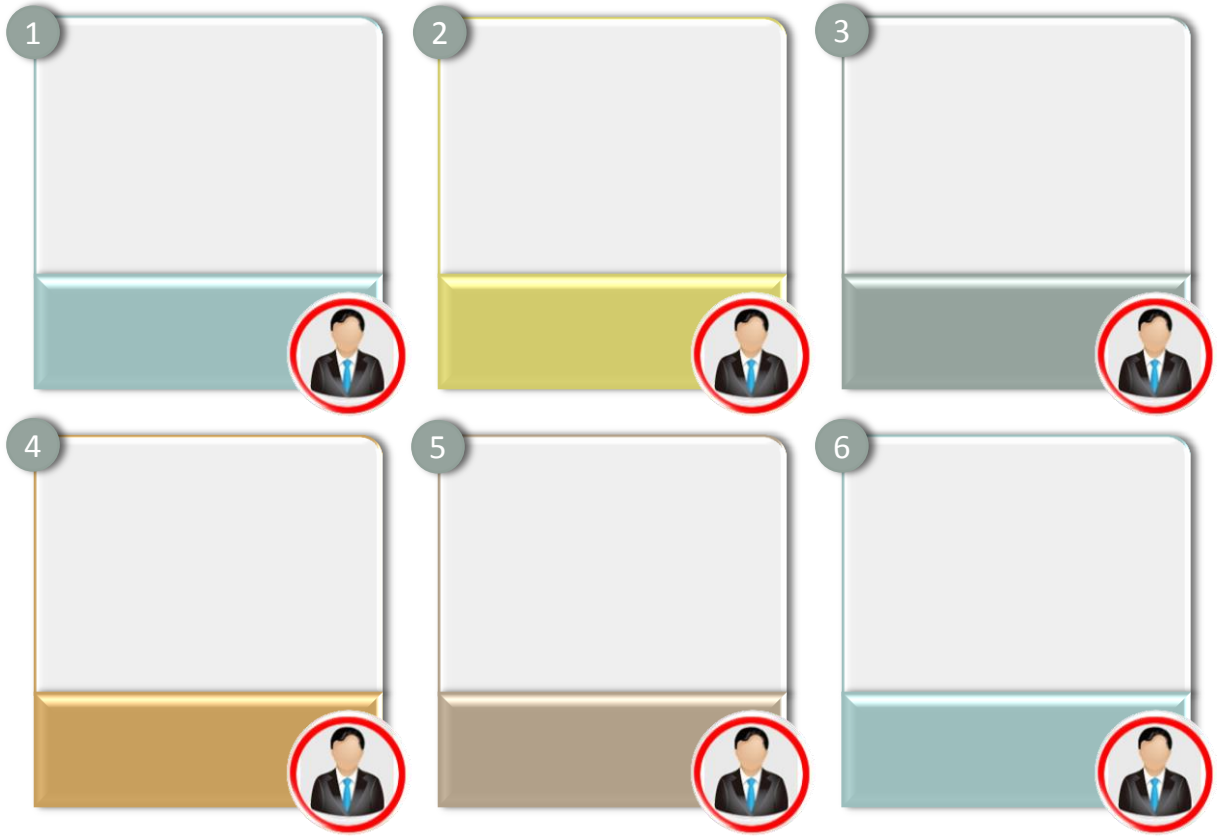
Aufgabe:

1. Kennzeichnen Sie die personenbezogenen Daten gemäß § 3 Abs. 1 BDSG
2. Kennzeichnen Sie die besonderen Arten pbD gemäß § 3 Abs. 9 BDSG
3. Erläutern Sie die Konsequenzen für die Betroffenen(Anhand der Schutzstufen)

Quelle: http://www.aachener-zeitung.de

Zusammenfassend

Welche Arten von pbD sind ohne Rechtsgrundlage nicht zu erfassen?



Welche pbD beinhalten besondere Risiken für die Betroffenen? **§ . Abs. .**
Begründen Sie dies: _____
_____
_____

Resümee, was sind Ihre vorrangigen Aufgaben als DSB?

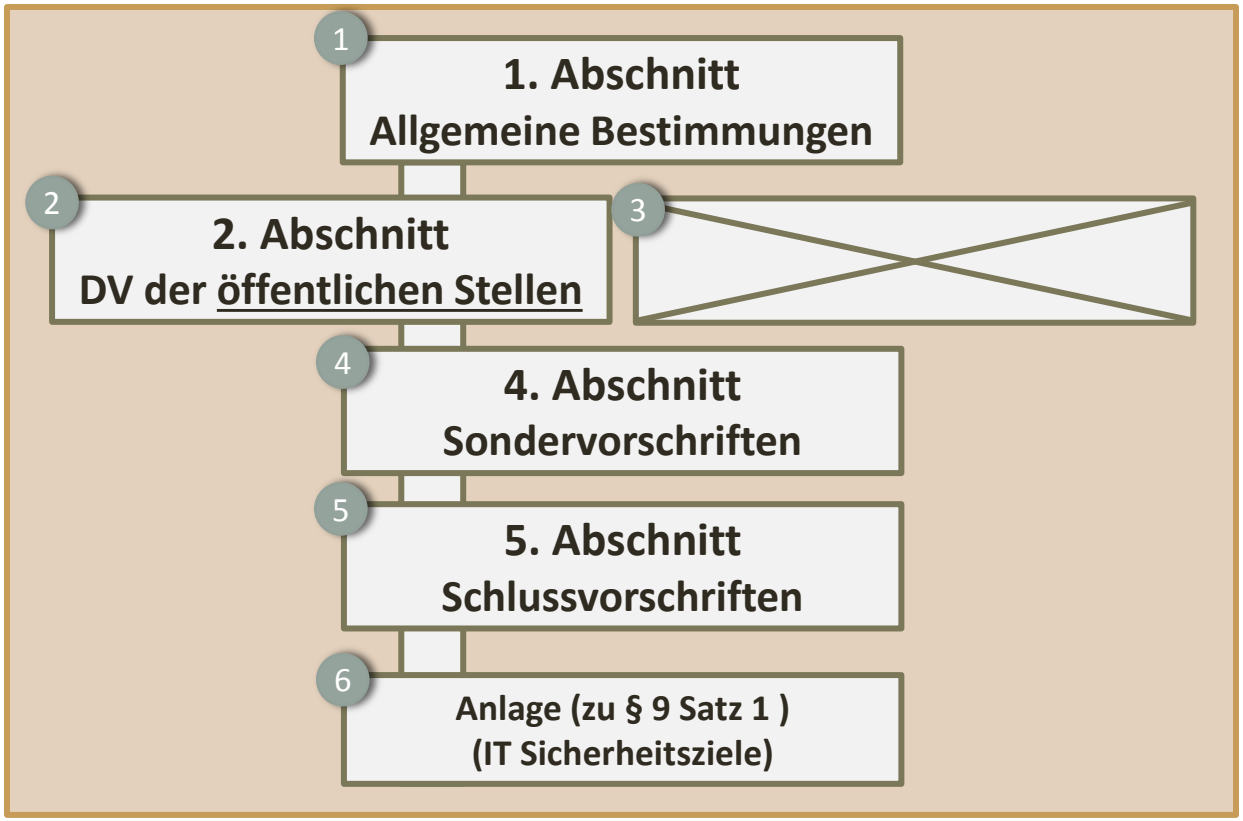
		J	N
1	Die Belange und Vorgaben der Geschäftsleitung umzusetzen?	☐	☐
2	Die Belange und Vorgaben Ihres Vorgesetzten umzusetzen?	☐	☐
3	Auf die ordnungsgemäße Anwendung der Datenverarbeitungs-programme, mit deren Hilfe personenbezogene Daten verarbeitet werden zu achten?	☐	☐
4	Die Belange und Vorgaben des IT-Leiters umzusetzen?	☐	☐
5	Auf das nicht erfassen von pbD gemäß § 3 Abs. 9 hinzuwirken?	☐	☐
6	Die Persönlichkeitsreche der Betroffenen zu wahren?	☐	☐
7	Sie schützen Daten natürlicher- und juristischer Personen?	☐	☐
8	Sie schützen Daten natürlicher Personen?	☐	☐
9	Sie wahren die Würde des Menschen durch Veranlassung von Berichtigung, Löschung und Sperrung der Daten bei der aut. DV?	☐	☐

Kreuzen Sie bitte die richtige Lösung an.

Die Systematik des BDSG

1

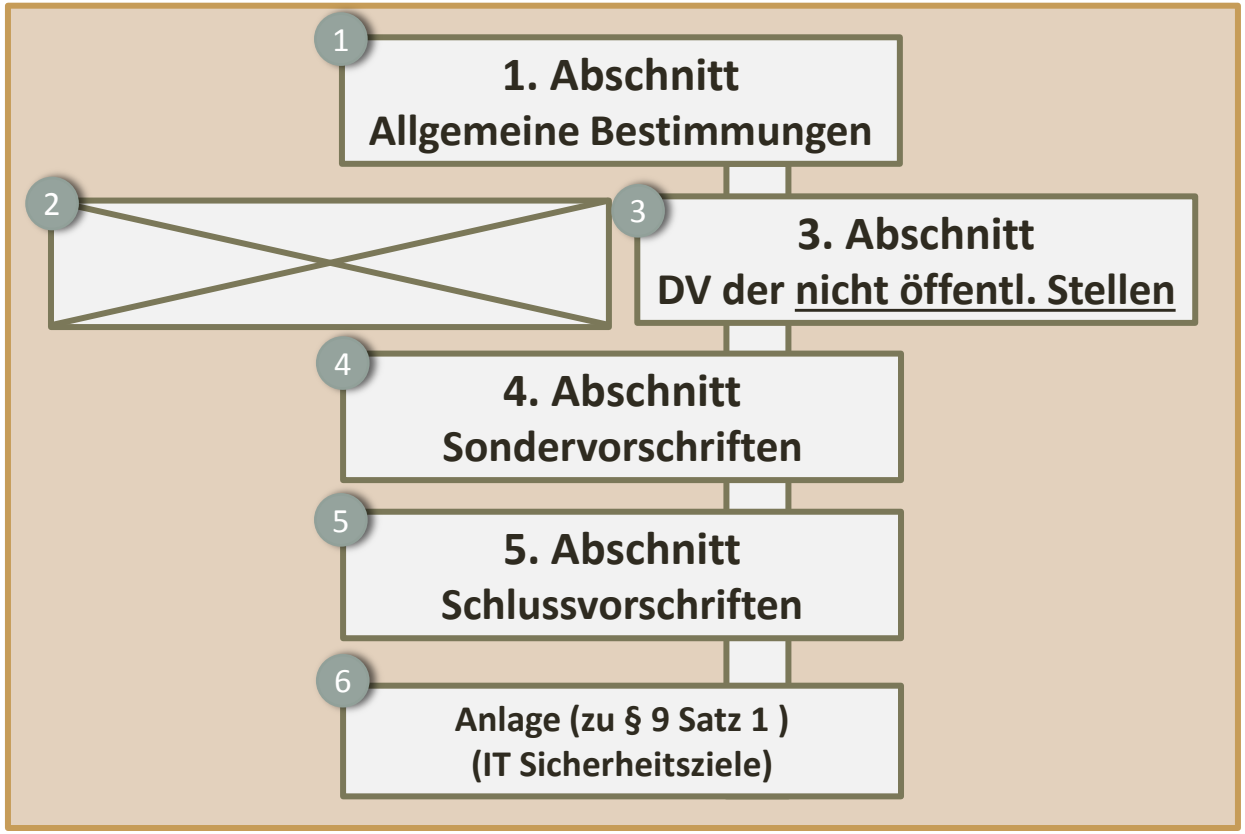
Die Regelungen des Bundesdatenschutzgesetzes (BDSG) für die **öffentliche Stellen** des Bundes(Behörden, Organe etc.)
(Vgl. § 2 Öffentliche und nicht-öffentliche Stellen Abs. 1 – 3 BDSG).



Die Systematik des BDSG

2

Die Regelungen des Bundesdatenschutzgesetzes (BDSG) für die **nicht öffentliche Stellen** - natürliche und juristische Personen.
(vgl. § 2 Öffentliche und nicht-öffentliche Stellen Abs. 4 BDSG).



Übungsaufgabe - Systematik des BDSG

2

Erster Abschnitt 1
§§ 1 – 11 Allg . . . . . und gemeins . . . Best . . . . . .

Zweiter Abschnitt 2
§§ 12 – 26 Datenver . . . . . der öffentl . . . . . St . . . . .

Dritter Abschnitt 3
§§ 27 – 38 Datenver . . . . . n . . . . öffentl . . . . . St . . . . .

Vierter Abschnitt 4
§§ 39 – 42 Sonderv . . . . . .

Fünfter Abschnitt 5
§§ 43 – 44 Schlussv . . . . . .

Sechster Abschnitt 6
§§45 – 46 Übergangsv . . . . . .

Anl . . . (z . § 9 S . . . 1)

Merke!!!

Historik des BDSG

1

Entwicklung des Bundesdatenschutzgesetzes (BDSG)

!

BDSG I von 1977 | **BDSG II von 1990** | **BDSG III von 2009**

1. **BDSG I von 1977**
   Schutz personenbezogener Daten vor Missbrauch der Beeinträchtigung schutzwürdiger Belange der Betroffenen bei der Datenverarbeitung

2. **BDSG II von 1990**
   Informationelles Selbstbestimmungsrecht (Volkszählungsurteil 1983)
   Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten

3. **BDSG III**
   International vergleichbarer Datenschutz
   Vorabkontrolle besonders sensibler Datenverarbeitungen

Übungsaufgabe - Historik zum BDSG(Teil 1 und 2)

Tragen Sie die verschiedenen BDSG – Novellen unten in das Schaubild ein.

Entwicklung des Bundesdatenschutzgesetzes (BDSG)

BDSG . von	**BDSG .. von . . . .**	**BDSG … von . . . .**

1 **BDSG . von 19 . .**
Schutz pers **. . . . . D . . . .** vor Missbrauch der Beeinträchtigung schutz . . . . . Belange der Betroff . . . . bei der Datenverarbeitung.

2 **BDSG .. von 19 . .**
Informa . . . . . Selbst . . . . . (Volkszählungsurteil 19. .)
Schutz des Einzelnen vor Beeinträchtigung seines Persönlich . . . . . beim Umgang mit personenb . . . . . Daten.

3 **BDSG … von 20 . .** beinhaltet E . -Datenschutzrichtlinie 9 ./4 ./E . **(19 . .)**
International vergl . . . . . Datenschutz
Vorab . . . . . besonders sen. . . . . Datenverarbeitungen

Übungsaufgabe - Rangordnung der Rechtsvorschriften

Vervollständigen Sie nachfolgende Begriffe/Bereichsspezifische Regelungen

EU R . . . . – Staatenverbund(28) – Wirtschafts- und Währungsunion

Anwendungsv . . . . . vor nationalem Recht bei Kollis . . .

Richtlinie 95/46/ . . des Europäischen Parlaments 1995 umgesetzt (2001)

Richtl . . . . für elektronische Kommunikation 2002/58/EG (2002)

C . . . . . der Grundrechte der EU (2000)

Grundgesetz(G.)

TK. | **TM.** | **UW.** | **SG.** | **BetrV.** | **T.**

Das Bundesdatenschutzgesetz(BD . . – ist subs . . . . .)

Die Landesdatenschutzgesetze(LD . . – sind subs . . . . .)

Gesetzesvorschriften und Normkörper

Ein vollständiges Zitat einer Gesetzes- bzw. einer Rechtsvorschrift besteht z.B. aus Artikel oder Paragraphenzeichen und der genau zitierten Norm.

Paragraph (bzw. Artikel), ggf. - Absatz, Nummer und Satz + Normkörper
z.B. **§** 4f **Abs.** 3 **S.** 4 **BDSG**
i.V.m. **§** 626 **Abs.** 1, 2 **BGB.**

Beachten Sie bitte, dass im GG keine Paragraphen, sondern Artikel verwendet werden. Ferner ist immer anzugeben, aus welchem Normkörper die zitierte Vorschrift stammt, also z.B. aus dem BGB oder aus dem BDSG…

Was besagt folgende Rechtsvorschrift? § 4d Abs. 5 Nr. 2 S. 1 BDSG

Unter welchem § finden Sie die Aufgaben des DSB und wann ein DSB bestellt werden muss? inkl. Normkörper.

Was besagt folgender Rechtsvorschrift? § 4f Abs. 1 S. 6 BDSG

Das IT-Grundrecht im Detail BVerfG (1 BvR 370/07, 1 BvR 595/07)

1

Zur dogmatischen Einordnung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die im nordrhein-westfälischen Verfassungsschutzgesetz (VSG) vorgesehene Online-Durchsuchung ist verfassungswidrig. Das entschied am 27. Februar 2008 das BVerfG (1 BvR 370/07, 1 BvR 595/07).

In seiner Entscheidung entwickelt das Gericht ein neues Grundrecht „auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“. Dieses Recht schützt den Betroffenen vor Zugriffen auf Computer, Netzwerke und vergleichbare Systeme, wenn diese Zugriffe sein Persönlichkeitsrecht gefährden.

1 Vertraulichkeit

IT Grundrecht

Vertraulichkeit und Integrität informationstechnischer Systeme.

2 Integrität

Nur die berechtigten Personen dürfen auf Informationen zugreifen

Informationen sind komplett, echt, unverändert, korrekt und unversehrt

Übungsaufgabe

1. Was besagt das „Informationelle Selbstbestimmungsrecht „ ?

2. Was bedeutet der Begriff „Normenklarheit“ ?

3. Was verstehen Sie unter dem Begriff „Schrankentrias“ ?

Merke!!!

Das BDSG ist ein Auffanggesetz, gemäß § 1 Abs. 3 S. 1

1

1. Der Datenschutz findet seine rechtlichen Grundlagen vor allem, aber nicht nur im Bundesdatenschutzgesetz (BDSG). Vielmehr dient dieses Gesetz als sogenanntes Auffanggesetz (**vgl. § 1 Abs. 3 S. 1**).

2. Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes(BDSG) vor - **Subsidiaritätsprinzip**.

3. Datenschutzrechtliche Vorschriften finden sich vor allem auch in **bereichsspezifischen Gesetzen** oder **bereichsspezifischen Regelungen** wieder z. B. dem:
   - A TKG – **Telekommunikationsgesetz**
   - B TMG – **Telemediengesetz etc.**

4. Diese gehen dann als speziellere Regelungen dem Bundesdaten-schutzgesetz vor**. Über sämtlichen nationalen Regelungen steht das Europäische Recht.**

Übungsaufgabe

1. Das Ulmer Urteil besagt das:

2. Was ist eine Rechtsnorm oder Rechtsvorschrift ?

3. In welchem Paragraphen im BDSG wird beschrieben, dass das BDSG subsidiär ist und was genau bedeutet dies ? Angabe inkl. Normkörper.

Datenschutzrechtliche Grundsätze

A **Subsidiaritätsprinzip**: Auffanggesetz - Bereichsrecht hat Vorrang!

B **Verbot mit Erlaubnisvorbehalt**: automatisierte Verarbeitung personenbezogener Daten benötigt ausdrückliche Gestattung!

C **Prinzip der Zweckbindung**: Erhebungsgründe bestimmen auch Verarbeitungs- und Nutzungsbefugnisse!

D **Prinzip der Transparenz**: Betroffener muss erkennen können, wie seine Daten automatisiert verarbeitet werden!

E **Verhältnismäßigkeitsprinzip**: Angemessene Zweck-Ziel-Relation bei der automatisierten Verarbeitung zu beachten!

F **Prinzip der Datensparsamkeit**: Personenbezug gering halten!

G **Sitzlandprinzip**: Entscheidend ist der Sitz der verantwortlichen Stelle (nicht der Ort der Verarbeitung)! Bsp. Facebook Urteil

Teilaspekte der Informationssicherheit

Anforderungen → **Informationen** ⇢ **Erwartungen**

Normative Anforderungen

- Verfügbarkeit
- Vertraulichkeit
- Integrität

Informationen

Login ins
Passwörter
Zugangs-Codes
Zugriffs-Codes
Unternehmensdaten
Kundenstamm
Lieferantenstamm
Personalstamm…

Erwartungen

- Authentizität
- Zurechenbarkeit
- Verbindlichkeit
- Verlässlichkeit

Zutrittskontrolle
zu Gebäuden und Serverräumen…

Zugangskontrolle
Authentifikation

Zugriffskontrolle
Berechtigungskonzept

Übungsaufgabe „Die drei Grundwerte der Informationssicherheit“

Vertr . . . . . .

Ver . . . . . .

Inte . . . . . .

Quelle: Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de

1. **Vertraulichkeit:** Vertrauliche Informationen müssen vor unb . . . . . Preisg . . . gesch . . . . werden.

2. **Verfügbarkeit:** Dem Benutzer stehen Dienstl . . . . . ., Funkt . . . . . eines IT-Systems oder auch Informationen zum geforderten Zeitp . . . . zur Verf . . . . . .

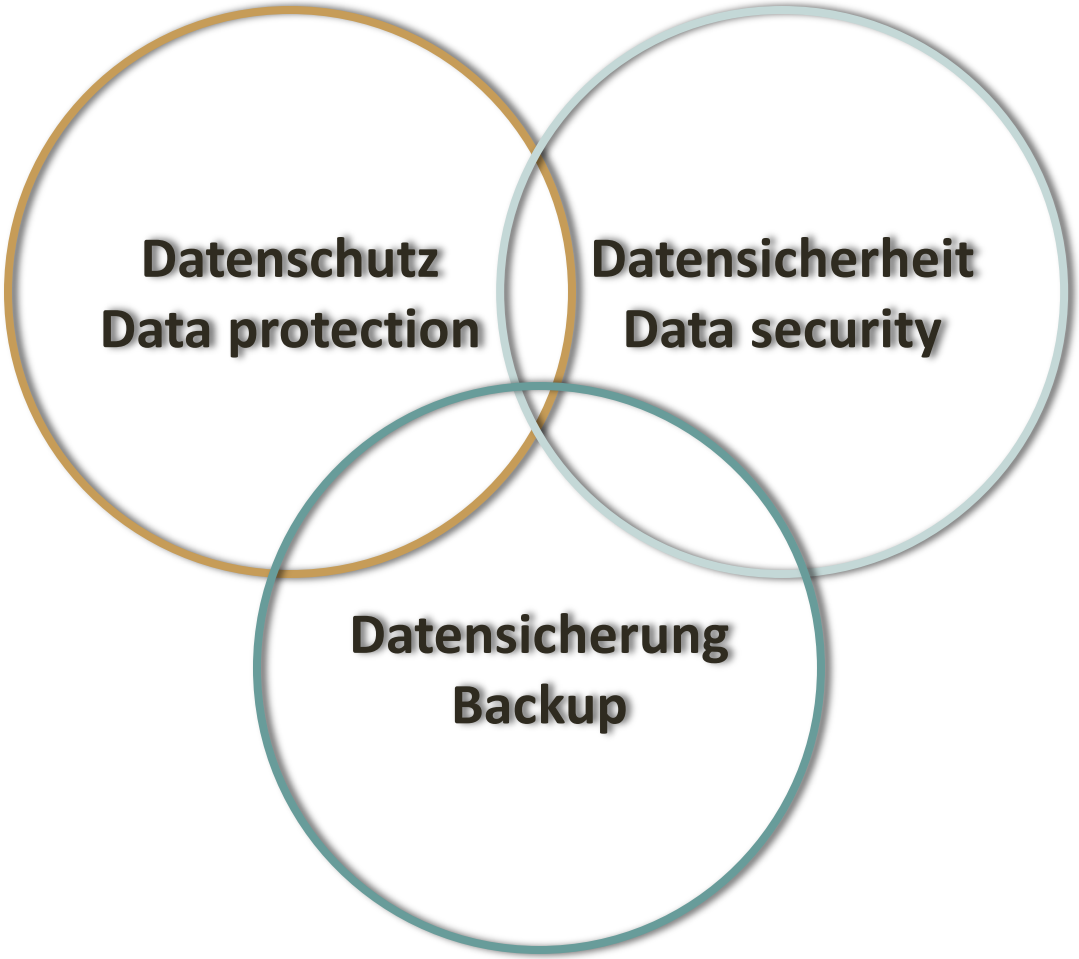
3. **Integrität:** Die Daten sind vollst . . . . . und unver . . . . . Der Begriff „Information“ wird in der Informationstechnik für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstell . . . zugeordnet werden können. Der Verlust der Integ . . . . . von Informat . . . . . kann daher bedeuten, dass diese unerlaubt veränd . . . wurden oder Angaben zum Autor verf . . . . . wurden oder der Zeitpunkt der Erstellung manip . . . . . wurde.

Auszug aus dem BSI/Grundschutz/Leitfaden/GS-Leitfaden

Datenschutz, Datensicherheit und Datensicherung

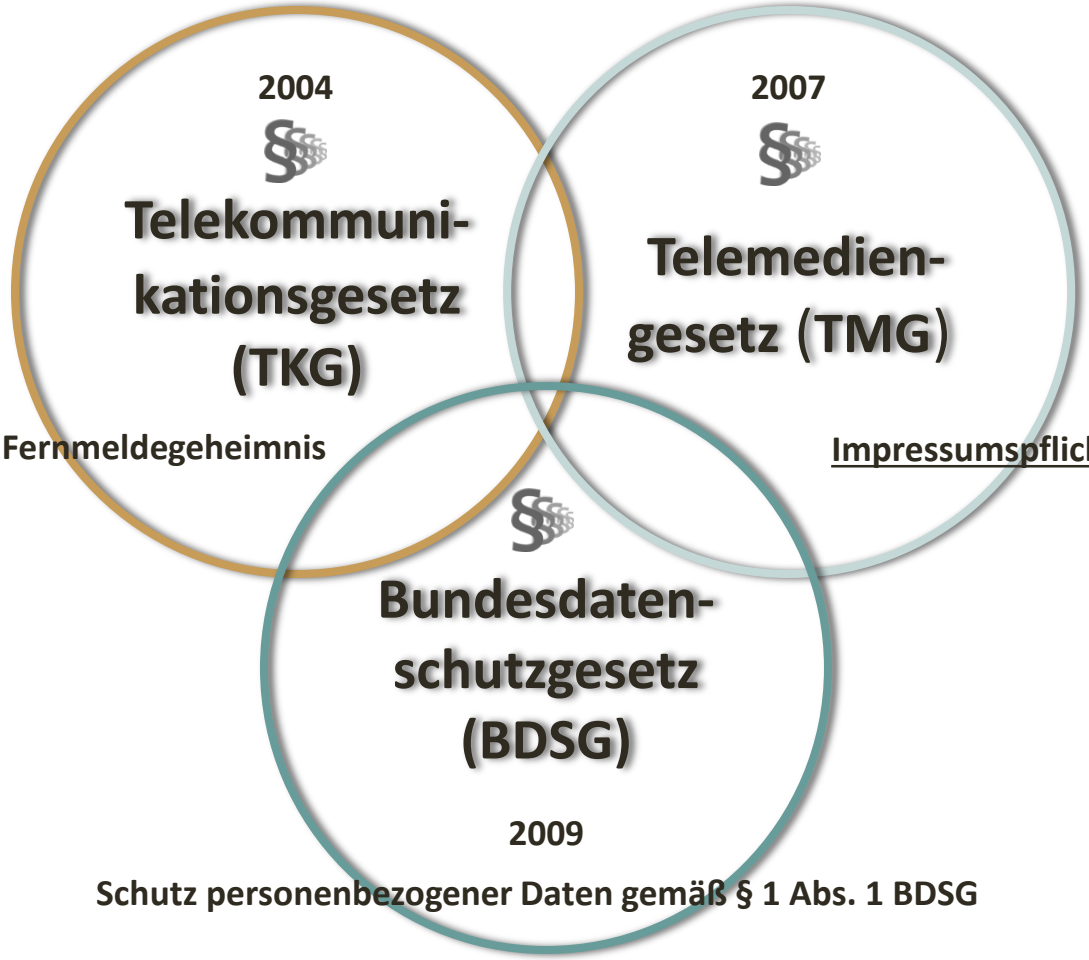
Obwohl die Zielsetzung der drei Bereiche unterschiedlich sind, sind sie nicht voneinander zu trennen. Da es in einigen Bereichen Überschneidungen gibt, sind die drei Bereiche am besten in ihrer Gesamtheit zu betrachten.

1



Der Dreiklang von TKG, TMG und BDSG

1



§ 88 Abs. 1 TKG Fernmeldegeheimnis

Impressumspflicht nach § 5 TMG

Schutz personenbezogener Daten gemäß § 1 Abs. 1 BDSG

TKG stand Mai 2012

Telekommunikationsgesetz (TKG)

Dem § 88 Fernmeldegeheimnis unterliegen z.B.

1. **Telefon**
2. **E-Mail**
3. **Fax**
4. **SMS**

§ 1 Zweck des Gesetzes

Zweck dieses Gesetzes ist es, durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.

§ 2 Regulierung, Ziele und Grundsätze

Abs. 1 Die Regulierung der Telekommunikation ist eine hoheitliche Aufgabe des Bundes…

§ 88 TKG und gesetzliche Archivierungspflichten

4

Gesetzliche Archivierungspflichten nach:

§ 257 HGB - Aufbewahrung von Unterlagen. Aufbewahrungsfristen
§ 147 AO - Ordnungsvorschriften für die Aufbewahrung von Unterlagen

A Buchführungsunterlagen, Jahresabschlüsse, Buchungsbelege etc. sind zehn Jahre lang aufzubewahren.

B Handelsbriefe und sonstige Unterlagen, die für die Besteuerung von Bedeutung sind, gemäß der AO sechs Jahre gespeichert werden.

Die Verletzung dieser gesetzlichen Aufbewahrungsfristen ist mit Geld- oder Freiheitsstrafe bis zu zwei Jahren (in besonderen Fällen höher) bedroht (§ 283 StGB). Taten sind jedoch nur bei vorsätzlichem, nicht jedoch bei fahrlässigem Handeln strafbar.

Private E-Mail-Nutzung:
Das Unternehmen unterliegt dann rechtlichen Pflichten aus dem Bundes-datenschutzgesetz (BDSG) und dem Telekommunikationsgesetz (TKG). Danach ist eine Überwachung und Speicherung(Archivierung) privater E-Mails nicht zulässig.

§ 88 TKG Fernmeldegeheimnis und Emails

6

Fallbeispiel

Ein Unternehmen stellt seinen Arbeitnehmer einen E-Mail-Account zur Verfügung.

Der Arbeitgeber gestattet es diesen E-Mail-Account auch für den privaten E-Mail-Verkehr zu nutzen.

In Folge eines Verdachtes will der Arbeitgeber auf die E-Mails des Arbeitnehmers zugreifen, weil dieser den Verdacht hegt es läge eine arbeitsvertragliche Verletzung des Mitarbeiters vor.

Dazu weist er den Systemadministrator an, das Postfach des Arbeitnehmers auszulesen und im Beisein des Arbeitgebers in Augenschein zu nehmen.

Begründung: Z. B. Verdacht auf Arbeitszeitbetrug oder Industriespionage .

Übungsaufgabe TKG, StGB

§ 88 Abs.1 TKG besagt ?

Unter welchem Pragrahen wird der Begriff „Diensteanbieter" im TKG beschrieben ?

Was ist unter dem Begriff „Diensteanbieter“ zu verstehen ?

Was ist unter dem Begriff „Anzeigepflicht“ zu verstehen ?

Unter welchem Pragrahen im TKG wird dieser erwähnt ?

Nach welchem Pragrahen im StGB „Nichtanzeige geplanter Straftaten“ wird dies geahndet ?

Wann wird ein Unternehmen zum „geschäftsmäßigen Diensteanbieter?

Was besagt § 206 Strafgesetzbuch ?

Anbieterkennzeichnung - Impressum gemäß TMG & RStV

1

Impressumspflicht nach § 5 TMG

Journalistisch-redaktioneller Inhalt nach § 55 Abs. 2 RStV

Impressumspflicht gemäß § 5 TMG

2

Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

Name des Unternehmens, § 5 Abs. 1 Nr. 1 TMG

Nr. 1 den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben zum Kapital gemacht werden, ist das Stamm- oder Grundkapital und der Gesamtbetrag der ausstehenden Einlagen anzugeben.
Bei nicht im Handelsregister eingetragenen Einzelunternehmen wird der Vor- und Zuname des Geschäftsinhabers anzugeben.

1

Angaben zur Kontaktaufnahme, § 5 Abs. 1 Nr. 2 TMG

Nr. 2 Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post - Emailadresse,

2

Angaben zur zuständigen Aufsichtsbehörde, § 5 Abs. 1 Nr. 3 TMG

Nr. 3 soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, z.B. nach § 34c GewO. Es sind Angaben zur zuständigen Aufsichtsbehörde anzugeben. Z. B. (Gewerbeerlaubnis gemäß § 34c GewO erteilt durch die Stadt Name, Ordnungsamt, Berufsaufsichtsbehörde gem. § 34c GewO: Ordnungsamt Ort, Vertretungsberechtigter: Vorname Nachname, Berufskammer: IHK Ort),

3

Impressumspflicht gemäß § 5 TMG

3

Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt …

Angabe von Registereintragungen, § 5 Abs. 1 Nr. 4 TMG

Nr. 4 das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer z.B.(HRB 0 18 15 X), **eine Steuernummer ist nicht anzugeben,**

4

Angaben im Falle reglementierter Berufe, § 5 Abs. 1 Nr. 5 TMG

Nr. 5 Reglementierte Berufe sind z.B. (Ärzte, Rechtsanwälte, Steuerberater…) oder bei welchen die Führung eines beruflichen Titels von bestimmten Voraussetzungen abhängig ist (z.B. Architekten, Ingenieure und fast alle Heilberufe). Notwendige zusätzliche Angaben sind: Zuständige Berufskammer, welcher der Diensteanbieter angehört, gesetzliche Berufsbezeichnung, der Staat, in dem diese Berufsbezeichnung verliehen wurde, jeweils geltende berufsrechtlichen Regelungen und wie diese zugänglich sind,

5

Angabe der Umsatzsteueridentifikationsnr. / Wirtschaftsidentifikationsnr. § 5 Abs. 1 Nr. 6 TMG

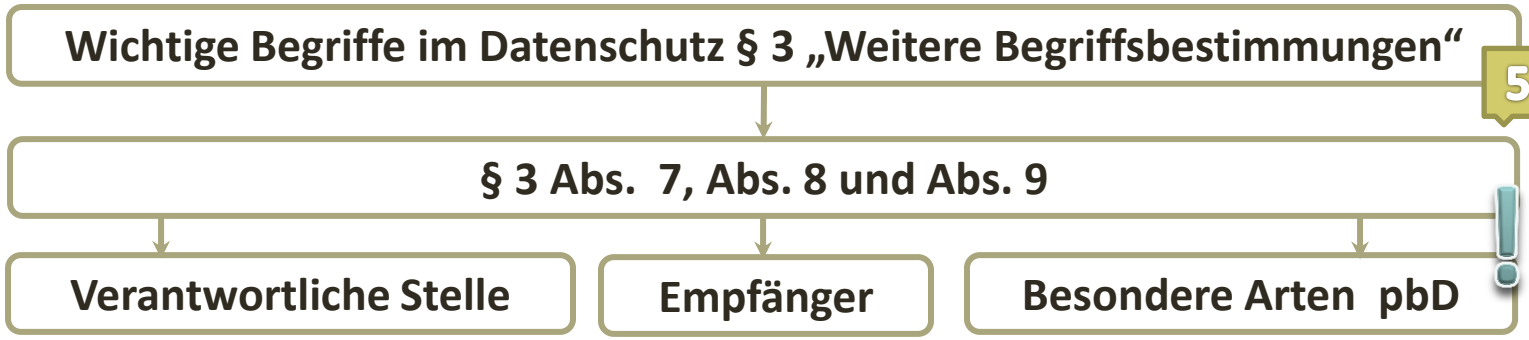
Nr. 6 in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer,

6

Abwicklung oder Liquidation, § 5 Abs. 1 Nr. 7 TMG

Nr. 7 Befindet sich eine AG, KGaA oder GmbH in Abwicklung oder Liquidation, ist dies angegeben.

7



Abs. 7 **Verantwortliche Stelle** ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Abs. 8 **Empfänger** ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

Abs. 9 **Besondere Arten personenbezogener Daten** sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschafts-zugehörigkeit, Gesundheit oder Sexualleben…

Pseudonymisierung § 3 Abs. 6a

1

Keine Pseudonymisierten Daten

Personenbezogene Daten gemäß § 3 Abs. 1 | Bes. Arten pbD § 3 Abs. 9

tbl_Patienten_Stammdaten

PNr	Vorname	Nachname	Strasse	Plz	Ort	E_Art1	E_Art2	E_Art3
1	Hans	Mustermann	Musterweg 4711	80000	München	Grippe	Angina	Fußpilz
2	Maria	Groß	Musterweg 4712	20000	Hamburg	Bronchitis	Grippe	

Pseudonymisierung - Definition

Pseudonymisieren – Verfahren:
Ein auf Personendaten angewendetes Verfahren, welches die Identifikations-merkmale z.B. Personendaten oder Krankheitsbilder einer Person in separaten Referenztabellen mit Schlüsselfeldern auslagert(Dritte Normalform). Klartext-Identifikationen sind wo immer möglich durch Anonymisierung oder der Pseudonymisierung zu ersetzen.
Der Zugriff auf die Daten erfolgt ausschließlich über die Schlüsselfelder. Da ein Schlüsselfeld z.B. die ErkrankungNr= 4711 noch nichts über die Art der Erkrankung aussagt, ist der Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren erfüllt - **Referenz-Pseudonyme.**

Übung

§ 4f Beauftragter für den Datenschutz
Wann muss ein Datenschutzbeauftragter bestellt werden?

Wenn mehr als .. Personen **st…..** Daten in **ni…** digitaler Form verarbeiten (vgl. § .f Abs. 1 Satz .). 1

Wenn mehr als . Personen **st….. automatisiert** Daten verarbeiten (vgl. § .f Abs. 1 Satz .). 2

Die Daten einer **Vor……. unterliegen** (vgl. § 4f Abs. 1 Satz 6, § 4d Abs. 5, § 3 Abs. .).
– Eingeschränkt!!! 3

Daten **geschäfts…..** zum Zweck der Überm……. verarbeitet oder Daten für Zwecke der M….- oder Meinungs…… automatisiert verarbeitet werden. 4

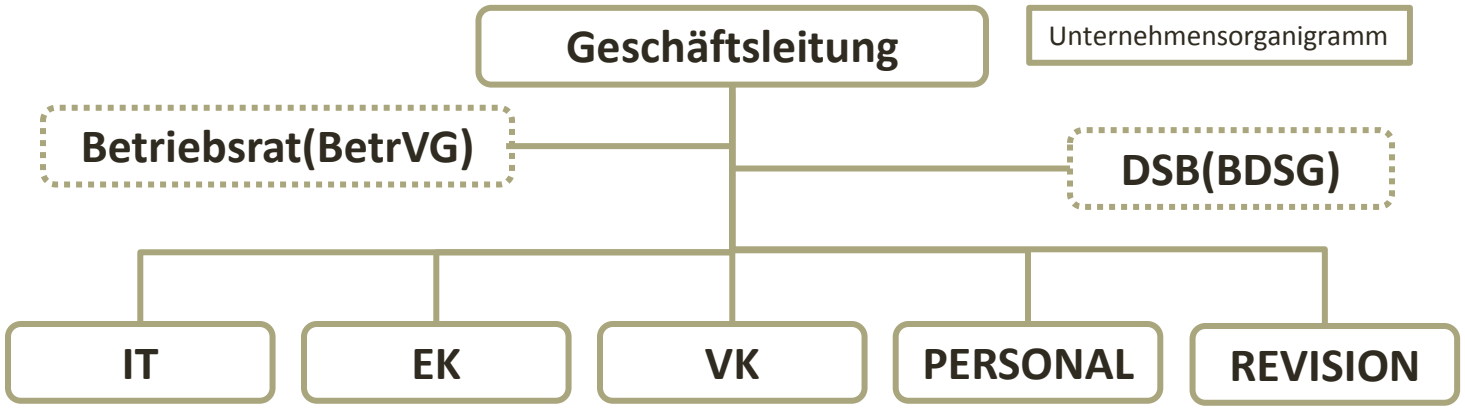
Stellung und Befugnisse des DSB

1

1. Die **unabhängige- und weisungsfreie Funktion** des Datenschutzbeauftragten, ist für seine Aufgabenerfüllung von ausschlaggebender Bedeutung (**vgl. § 4f Abs. 3 Satz 2).**

2. In seiner Funktion als Datenschutzbeauftragter ist der Datenschutzbeauftragte gemäß **§ 4f Abs. 3 Satz 1** dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen – (**Stabsstelle**).

3. Er darf bei der Wahrnehmung seiner Aufgaben **nicht** den Weisungen der nicht-öffentlichen Stelle unterliegen**,** er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes **weisungsfrei.**



Besondere Arten von pbD § 3 Abs. 9

2

Folgende Datenarten sind besondere Arten von personenbezogenen Daten und unterliegen der Vorabkontrolle!

1. **rassische und ethnische Herkunft** (z. B. Hautfarbe, Volksgruppe, „Asiate“, „Zigeuner“, „Mischling“)
2. **politische Meinungen** (z. B. Mitgliedschaften in Parteien, Teilnahme an Demonstrationen, „konservativ“, „links“)
3. **religiöse oder philosophische Überzeugungen** (z. B. Mitgliedschaft in einer Kirche oder Sekte, Atheist, „isst kein Schweinefleisch“)
4. **Gewerkschaftszugehörigkeit** (z. B. als Mieter einer Gewerkschaftswohnung oder Abonnement einer entsprechenden Zeitschrift)
5. **Gesundheit** (alle Angaben über körperliche und geistige Zustände und Bewertungen, z. B. Schwerbehinderung, Krankheiten, Schwangerschaft, Medikamenten/Drogen Gebrauch, genetische Daten, körperliches Erscheinungsbild)
6. **Sexualleben** (z. B. Kunde eines Erotik Händlers, „lesbisch“, „schwul“, „Viagra - Käufer“,)

Wenn besondere Arten von personenbezogenen Daten vorliegen, dann gelten für sie in einigen Bereichen strengere Vorgaben. Welche Bereiche dies sind, ergibt sich jeweils direkt aus dem Gesetzeswort laut des BDSG.

Vgl. § 4a Abs. 3 BDSG(Einwilligung), § 4d Abs. 5 BDSG(Vorabkontrolle) und § 28 Abs. 6 bis 9 BDSG(spezielle Vorschriften).

Verfahrensverzeichnisse und Meldepflichten gegenüber den Datenschutzaufsichtsbehörden - § 4d BDSG(MP)

2

Die Verfahren automatisierter Datenverarbeitung, in denen personenbezogene Daten geschäftsmäßig

zum Zweck der anonymisierten Übermittlung gemäß § 30 BDSG, gespeichert werden, unterliegen ohne Ausnahme der Meldepflicht (§ 4 d Abs. 4 BDSG).
Wissenschaftliche Zwecke, Forschungsdaten.

Unerlässlicher Bestandteil der Anonymisierung ist in jedem Falle die Löschung der expliziten bzw. direkten Identifikationsmerkmale wie Namen und Anschriften, Email usw.

§ 30a BDSG - Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung

Markt- und Meinungsforschungsinstitute, erheben z. B. Daten wie:
Einsichten, Einstellungen, Stimmungen oder Wünsche der Bevölkerung, Wahl – Prognosen etc.

Eine Meldepflicht der Verfahrens-verzeichnisse, aufgrund dieser sensiblen Daten

besteht immer!

§ 4e Inhalt der Meldepflicht i.V.m. § 4g Abs. 2 S. 2

5

§ 4e Inhalt der Meldepflicht
Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 plus Anlage zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

Nr. 9 ist nicht öffentlich, sondern im Unternehmensverfahrensverzeichnis auszuweisen!

Übung - Aufgaben des Datenschutzbeauftragten

		J	N
1	Der Beauftragte für den Datenschutz wirkt auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hin?	☐	☐
2	Der Beauftragte für den Datenschutz kann sich in Zweifelsfällen an die zuständige Landesdatenschutzbehörde wenden - nach § 38 Abs. 1 S. 2	☐	☐
3	Er hat insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen?	☐	☐
4	Der Datenschutzbeauftragte schult das Personal, das im Umgang mit pbD tätig ist, mit den Vorschriften des Datenschutzes?	☐	☐
5	Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar	☐	☐
6	Der Datenschutzbeauftragte ist letztendlich verantwortlich für den Datenschutz?	☐	☐
7	Der Datenschutzbeauftragte ist für die Datensicherung(Backup) verantwortlich?	☐	☐

Was ist ein Konzern?

§ 18 Konzern und Konzernunternehmen, Aktiengesetz(AktG.)

(1) Sind ein herrschendes und ein oder mehrere abhängige Unternehmen unter der einheitlichen Leitung des herrschenden Unternehmens zusammengefasst, so bilden sie einen Konzern; die einzelnen Unternehmen sind Konzernunternehmen.

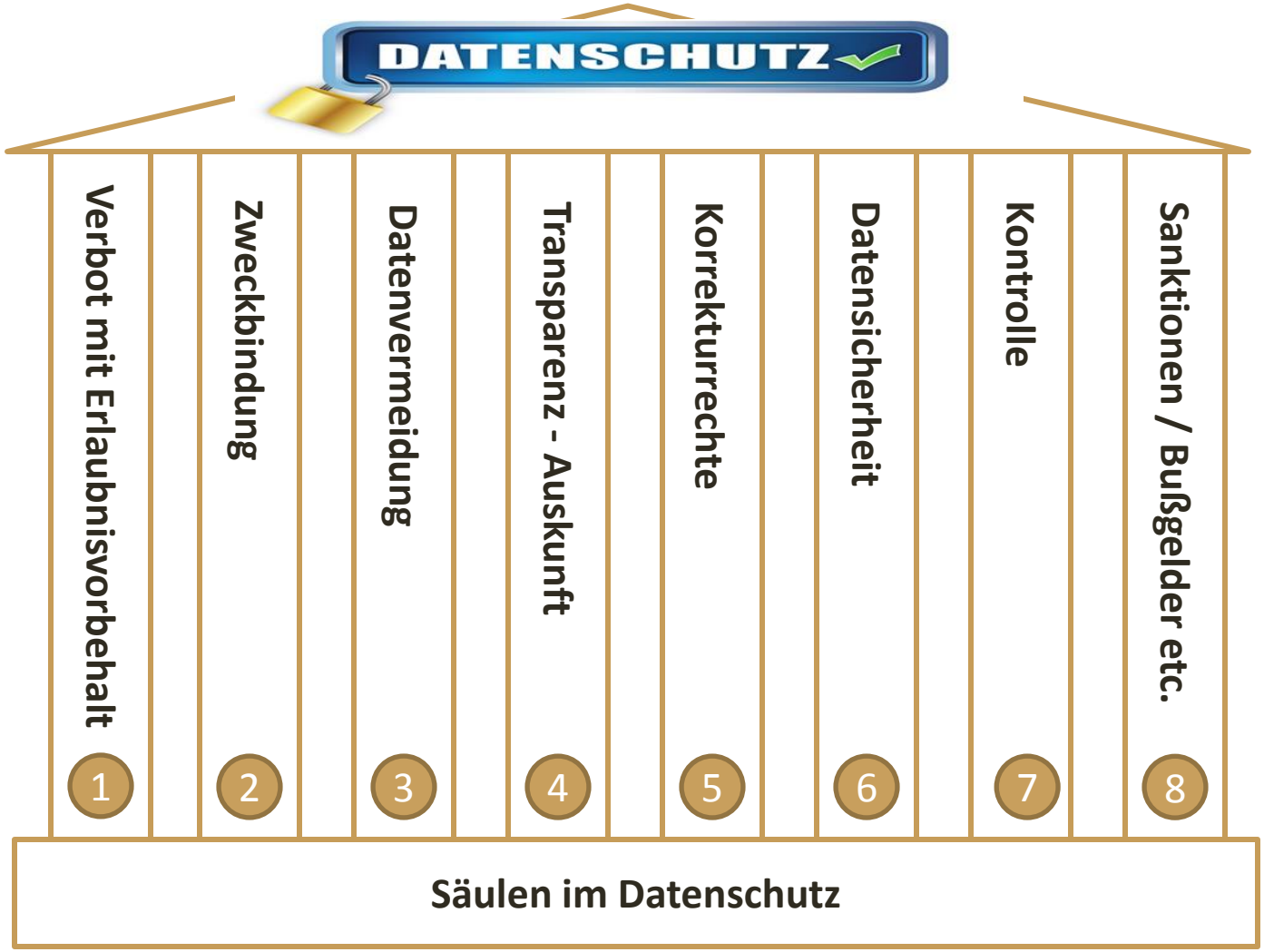
(2) Sind rechtlich selbständige Unternehmen, ohne dass das eine Unternehmen von dem anderen abhängig ist, unter einheitlicher Leitung zusammengefasst, so bilden sie auch einen Konzern; die einzelnen Unternehmen sind Konzernunternehmen.

Mehrfachtätigkeit als Datenschutzbeauftragter

Ein Spezialfall des Konzerndatenschutzbeauftragten stellt die Mehrfachtätigkeit eines Datenschutzbeauftragten dar. Hier ist ein **externer Datenschutzbeauftragter** gleichzeitig für mehrere Unternehmen einer Gruppe oder eines Konzerns tätig.
Im Bereich der Konzernmutter kann dieser z.B. als betrieblicher DSB bestellt werden.

Ein Datenschutzbeauftragter kann auch für mehrere Unternehmen eines Konzerns bestellt werden – eine Mehrfachtätigkeit ist als externer DSB zulässig und üblich!

Die acht Grundprinzipien des Datenschutzes



In Anlehnung an Quelle: GDD-Datenschutz-Jahrbuch 2013

1	**Verbot mit Erlaubnisvorbehalt** Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist grundsätzlich verboten! Das ist ein Grundsatz des BDSG. Eine Ausnahme besteht nur dann, wenn es eine andere Rechtsvorschrift erlaubt oder Sie freiwillig in die Verarbeitung Ihrer Daten eingewilligt haben. **§ 4 Abs. 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.	**§ 4**
2	**Zweckbindung** Jeder Datenverarbeitung muss ein bestimmter Zweck zugrunde liegen. Der Zweck muss vor der Verarbeitung festgelegt und dokumentieret worden sein. **§ 14 Abs. 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.	**§ 14** **§ 28** **§ 31** **etc.**

5

EuGH kippt Kopplungsverbot

Die Verknüpfung von Gewinnspielen mit dem Einkauf von Waren ist nicht automatisch wettbewerbswidrig, urteilt der Europäische Gerichtshof. Das deutsche Kopplungsverbot ist damit Geschichte.

Stein des Anstoßes: Die "Millionenchance" von Plus brachte das Verfahren ins Rollen.

Der Europäische Gerichtshof (EuGH) hat in einem Grundsatzurteil das sogenannte Kopplungsverbot des deutschen Wettbewerbsrechts für europarechtswidrig erklärt.

Das grundsätzliche Verbot die Teilnahme an einem Preisausschreiben oder Gewinnspiel von dem Erwerb einer Ware abhängig zu machen, lässt sich nicht mit der EU-Richtlinie über unlautere Geschäfts-praktiken vereinbaren, entschied das Gericht.

§ 4a Einwilligung

Welche Voraussetzungen stellt das BDSG an eine gültige Einwilligungserklärung?

1	**Einwilligung muss auf freier Entscheidung beruhen, also ohne Zwang gemäß (§ 4a Abs. 1 Satz 1 i.V.m. § 28 Abs. 3b) – Kopplungsverbot!**
2	**Es ist auf den Zweck der Verarbeitung hinzuweisen. (§ 4a Abs. 1 Satz 2).**
3	**Es ist auf die Folgen der Verweigerung der Einwilligung hinzuweisen. (§ 4a Abs. 1 Satz 2).**
4	**Einwilligung muss schriftlich erfolgen gemäß (§ 4a Abs. 1 Satz 3). Bei nicht-öffentlichen Stellen i.V.m. (§ 28 Abs. 3a und i.V.m. § 13 Abs. 2 TMG).**
5	**Erklärung, ist im Erscheinungsbild hervorzuheben. Einwilligung muss gut erkennbar sein (§ 4a Abs. 1 Satz 4 i.V.m. § 28 Abs. 3a).**
6	**Werden besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt muss dies ausdrücklich erklärt werden (§ 4a Abs. 3).**
7	**Ausnahme zu Punkt 6 im Bereich der wissenschaftlichen Forschung gemäß (GG Art. 5 Abs. 3) i.V.m. (§ 4a Abs. 2 Satz 1 und § 4a Abs. 2 Satz 2).**

Auftragsdatenverarbeitung

4

4 Der Dienstleister ist weisungsgebunden in Bezug auf die Datenverarbeitung. Der Auftraggeber schreibt dem Dienstleister exakt vor, wie er mit den Daten umzugehen hat.

Auftragnehmer im Sinne § 11 BDSG sind oft folgende Unternehmen:

A **Callcenter**

B **Aktenvernichter**

C **Schreibbüro**

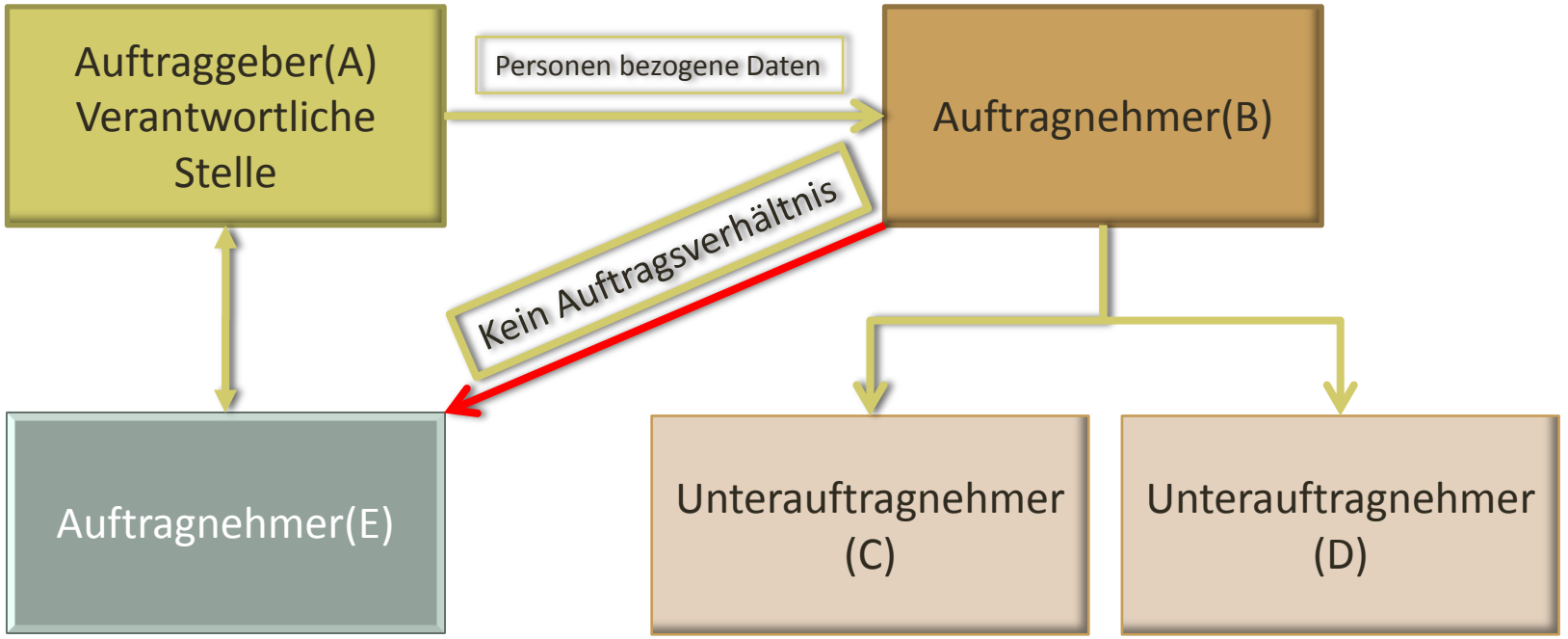
D **Lettershop**

E **Archivierungsdienstleister**

F **Externe Systemadministratoren (nach § 11 Abs. 5 BDSG)**

G **Wartung und Fernwartung von EDV Geräten durch externe Firmen**

Auftragsdatenverarbeitung gemäß § 11 BDSG
Schematischer Datenfluss zwischen den Unternehmen



Beschreiben Sie die Auftragsverhältnisse gemäß § 11 BDSG zwischen den Unternehmen. 1

Auftraggeber(A) bittet Auftragnehmer(B) die Daten an Auftragnehmer(E) zu übersenden, ist die zulässig? 2

Informationspflicht § 42a

2

Es muss sich dabei um personenbezogene Daten handeln, die aus einer der folgenden Kategorien stammen:

Besondere Arten von personenbezogenen Daten gemäß § 3 Abs. 9 BDSG
(etwa Gesundheitsdaten oder Religions / Gewerkschaftszugehörigkeit) etc.

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. Daten, die einem Berufsgeheimnis unterliegen (z. B. von einem Arzt oder RA …)
3. Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht darauf beziehen
4. Daten zu Bank oder Kreditkartenkonten

3. Für den Betroffenen müssen aufgrund der Panne schwerwiegende Beeinträchtigungen drohen, etwa finanzielle Schäden bei Kreditkarten-Informationen oder die Gefahr eines Identitätsdiebstahls.

Anlage zu § 9 (Technische und organisatorische Maßnahmen) – Nr. 1 bis 8

1 **Zutrittskontrolle** zu Gebäuden und Serverräumen... **§ 9 plus Anlage Nr. 1**

2 **Zugangskontrolle** Authentifikation **§ 9 plus Anlage Nr. 2** Benutzername und Passwort, Firewalls...

3 **Zugriffskontrolle** Berechtigungskonzept **§ 9 plus Anlage Nr. 3** Verschlüsselungsverfahren mit Passwort...

4 **Weitergabekontrolle**(SSL, VPN...)

5 **Eingabekontrolle**(Protokolldatei...)

6 **Auftragskontrolle**(gem. § 11 BDSG)

7 **Verfügbarkeitskontrolle**(Backups...)

8 **Zwecktrennungsgebot** (Zweckb.)

Anlage (zu § 9 Satz 1) IT – Sicherheit

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

Anlage (zu § 9 Satz 1), Verfügbarkeitskontrolle Nr. 7

7

Wichtige Sicherheitsmaßnahmen zur Verfügbarkeitskontrolle sind z.B.:

A Tägliche Erstellung von Sicherungskopien - Backups
B Erprobtes Konzept zur Rekonstruktion der Datenbestände(Recovery)
C Sichere Aufbewahrung der Sicherungskopien an ausgelagertem Ort
D Einsatz von gespiegelten Festplatten z.B. RAID Systemen
E Verwendung von Tresoren für Sicherungskopien
F Notfallplan nach BSI-Standard 100-4 / 101-1 ISMS(IT-Grundschutz)…
G Unterbrechungsfreie Stromversorgung (USV) und Notstromaggregat
H Meldesysteme für Rauch, Feuer und Wasser…
I Gasbasiertes Brandlöschsystem und andere Feuerlöscheinrichtungen
J Video- und Alarmanlage zur Diebstahlsicherung (EN-1627 / EN-1630)
K Schutz–Steckdosenleisten, Überspannungss., Kabelverl. n. DIN(18015)
L Klimaanlage, Klimatisierung nach ETS 300019, Temp. zw. 18 und 25 °C
M Brandschutztüren, Brandschutzwände (F90)

Nur autorisiertes Personal hat über die Identifikation mit anschließender Authentifikation zutritt zu Serverräumen und zum Datenarchiv!

Über das BSI

1

A **BSI steht für?**
Bundesamt für Sicherheit in der Informationstechnik

B **Was macht das BSI?**
Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen

C **Die IT-Grundschutz-Standards**

1. BSI-Standard 100-1: Managementsysteme für Informationssicherheit(ISMS)
2. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
3. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
4. BSI-Standard 100-4: Notfallmanagement

Urheberrechte - Bildernachweis

Alle Bilder welche zur optischen Unterstützung des Lernenden im Seminar: „betrieblicher Datenschutzbeauftragter gemäß §§ 4f, 4g BDSG“ dienen, wurden erworben bei Fotolia.com

http://de.fotolia.com/id/45001493
http://de.fotolia.com/id/27195025
http://de.fotolia.com/id/29437951
http://de.fotolia.com/id/33652250
http://de.fotolia.com/id/34053562
http://de.fotolia.com/id/38818944
http://de.fotolia.com/id/37944046
http://de.fotolia.com/id/48979689
http://de.fotolia.com/id/20188400
http://de.fotolia.com/id/46162734
http://de.fotolia.com/id/38751832
http://de.fotolia.com/id/19111399

Quellangaben:

Bundesdatenschutzgesetz - BDSG III von 2009, Datenschutz von A bis Z (Haufe), beck-online.beck.de, Dr. Wilfried Grieger, Seminar zum Kommunikationsrecht Prof. Dr. Gersdorf, Hajo Köppen Datenschutz A bis Z.