Vorlesung Datenschutzrecht

TU Dresden Sommersemester 2018

RA Dr. Ralph Wagner LL.M.

Agenda 19.04.2018

I. Organisatorisches
II. Literaturempfehlung
III. Einführung in den Datenschutz und das Datenschutzrecht
    1. Grundlagen
        a. Historisches zum Datenschutzrecht
        b. Anknüpfungspunkte in der Gegenwart
        c. Datenschutz als Persönlichkeitsrecht
        d. Datenschutzreform in Europa
        e. Die Datenschutzgesetze
        f. Anwendungsbereich des Datenschutzes
    2. Beteiligte Personen

I. Organisatorisches

- Kontakt
- Termine: 19.04.2018; 03.05.2018; 17.05.2018; 31.05.2018; 14.06.2018; 18.06.2018; 12.07.2018
- Ziele, Klausur
- Literatur, Zeitschriften, Fundstellen

II. Literaturempfehlung

Kommentare (Auswahl)

- Ehmann/Selmayr: Datenschutz-Grundverordnung: DS-GVO, 2. Auflage 2018,
- Gola: Datenschutz-Grundverordnung VO (EU) 2016/679: DS-GVO, 2. Auflage 2018
- Paal/Pauly: Datenschutzgrundverordnung/ Bundesdaten-schutzgesetz: DS-GVO/BDSG, 2. Auflage 2018
- Schwartmann/Jaspers/Thüsing/Kugelmann: Datenschutz-Grundverordnung mit Bundesdatenschutzgesetz

Lehrbücher (Auswahl)

- Roßnagel (Hrsg.), Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze; 1. Auflage 2017
- Rüpke/v. Lewinski/ Eckhardt, Datenschutzrecht – Grundlagen und europarechtliche Neugestaltung; 1. Auflage 2018
- Schantz/Wolff, Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis; 1. Auflage 2017

Zeitschriften (Auswahl)

- Datenschutzberater
- Datenschutz und Datensicherheit (DuD)
- Recht der Datenverarbeitung (RDV)
- Zeitschrift für Datenschutz (ZD)

III. Einführung in den Datenschutz und das Datenschutzrecht

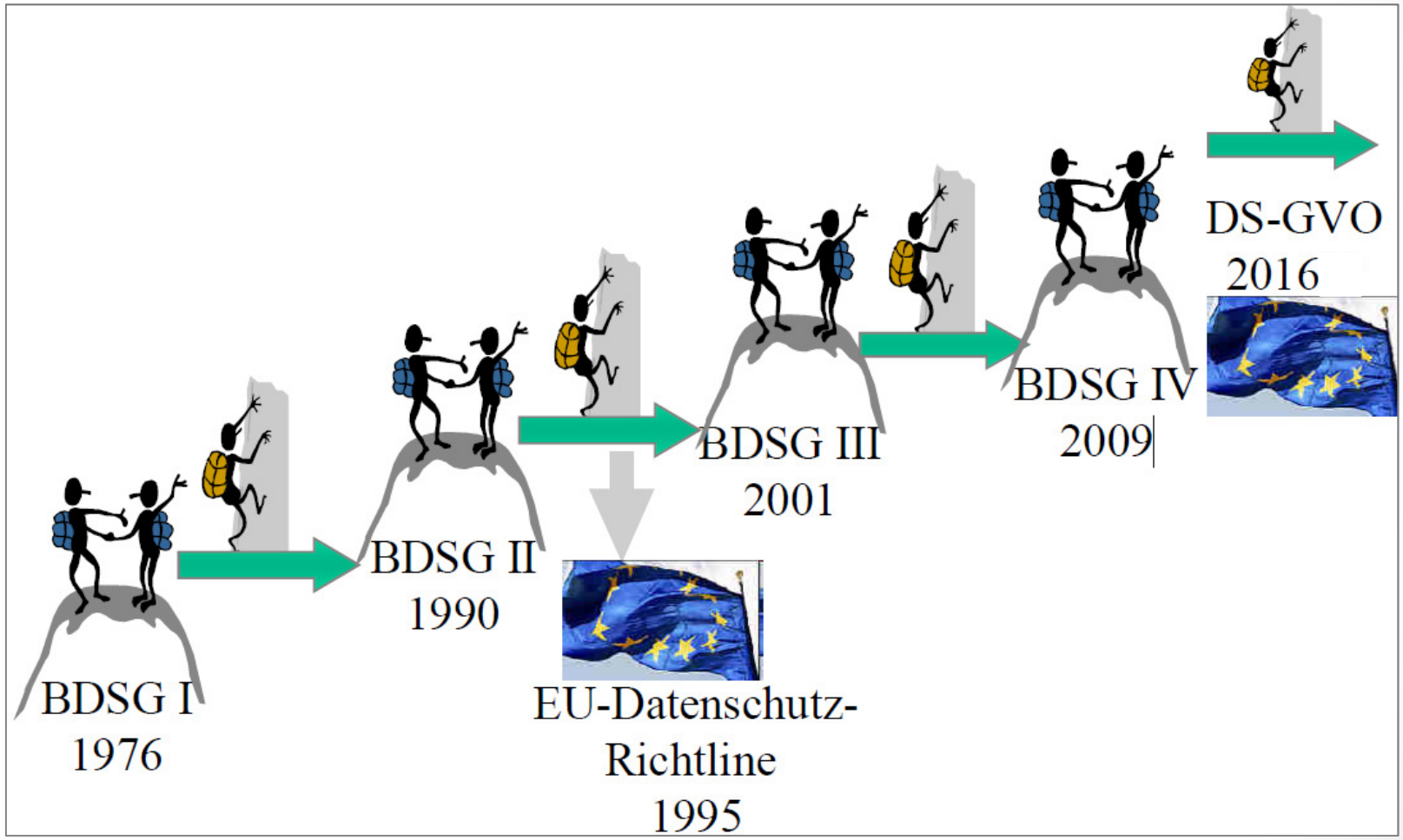
1. Grundlagen

a. Historisches zum Datenschutz

Zeitalter „vor der EDV“

- uralte Datenschutz-Bereiche: Priester, Ärzte, Anwälte
- Unverletzlichkeit der Wohnung (Schutz der Privatsphäre)
- Post- und Briefgeheimnis
- Fernmeldegeheimnis

„EDV Zeitalter“



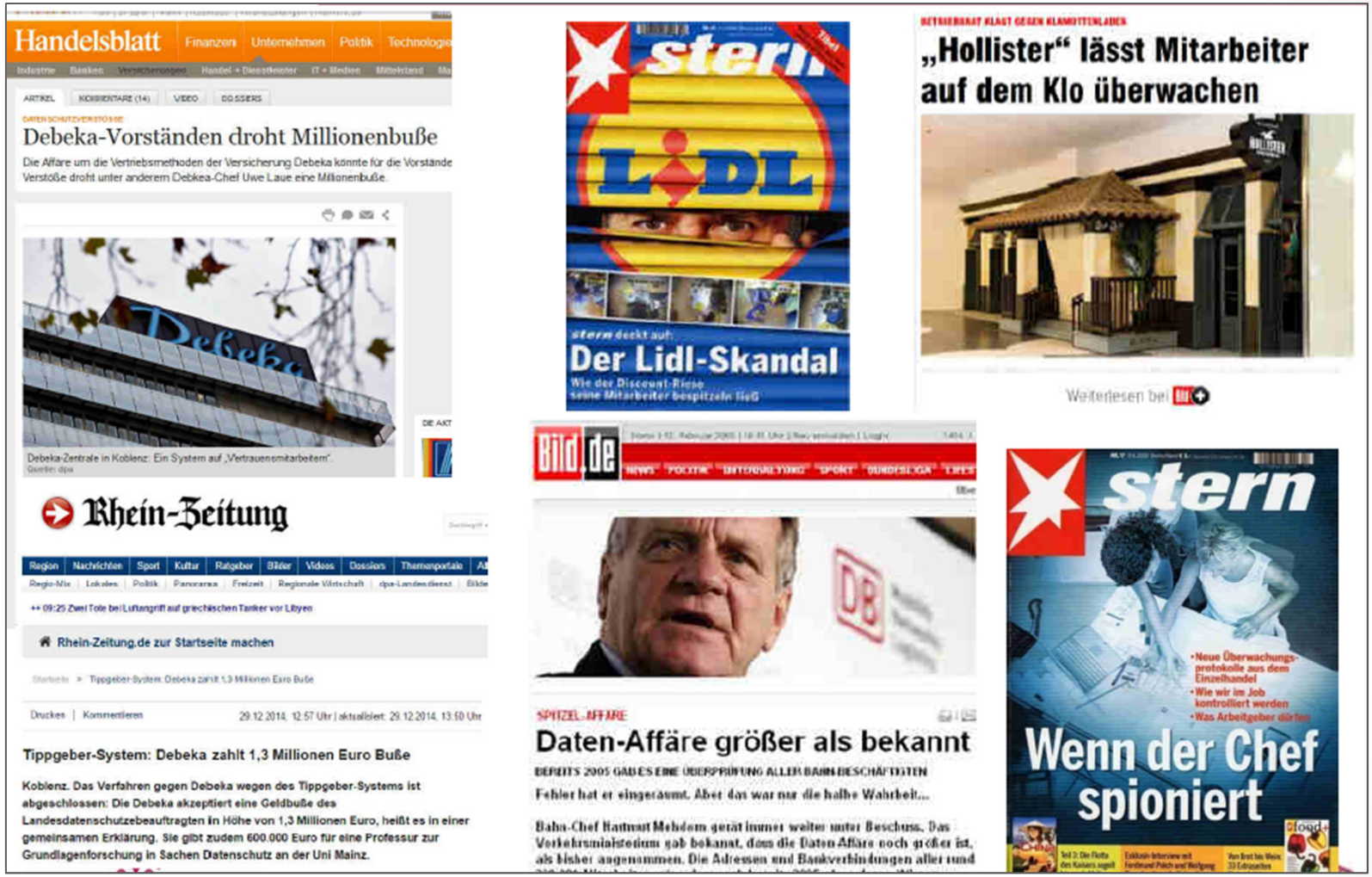
b. Anknüpfungspunkte in der Gegenwart

- Die fortschreitende technische Entwicklung in der **automatisierten Datenverarbeitung führt zu steigenden Gefahren des Datenmissbrauchs**.

- Es fallen immer mehr Daten an, die nahezu unbegrenzt gespeichert, verknüpft und ausgewertet werden können.

- Der Einzelne wird dadurch in seinen **Persönlichkeits- und Freiheitsrechten** beeinträchtigt, insbesondere wenn er nicht weiß, wer welche Daten über ihn hat, was dieser mit ihnen macht und an wen er sie weitergibt.

- Begriff des Datenschutzes wird heutzutage oft medial gebraucht
- dabei geht es meist um Skandale und ungenügenden Datenschutz
  - Beispiele dafür sind: Affäre um Edward Snowden oder ständige Meldungen über mangelnden Datenschutz bei Windows, WhatsApp oder Facebook



Datenschutzskandale

Warum geben wir solche Daten überhaupt weg?

- unserem Arbeitgeber?
- z.B. für den Online-Einkauf, Newsletter-Abos
- oder um in Kontakt zu bleiben

„weil wir leben“

c. Datenschutz als Persönlichkeitsschutz

Informationsbedürfnis:

- Arbeitgeber →
- Finanzamt →
- Geschäftspartner →
- Soziale Netzwerke →
- Versicherungen →
- Banken →

Persönlichkeitsrechtsschutz:

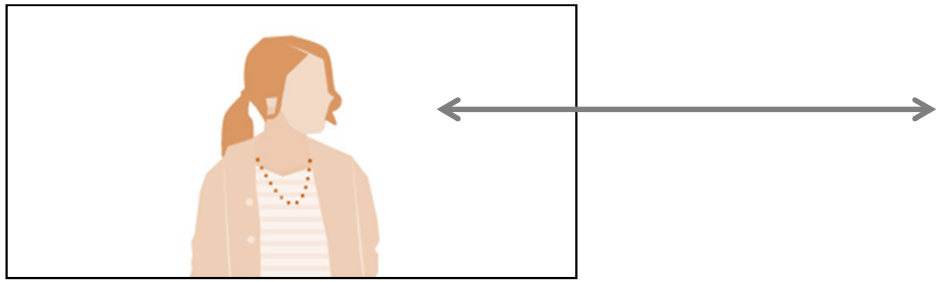
Der Einzelne soll wissen,

wer | was | wann | bei welcher Gelegenheit

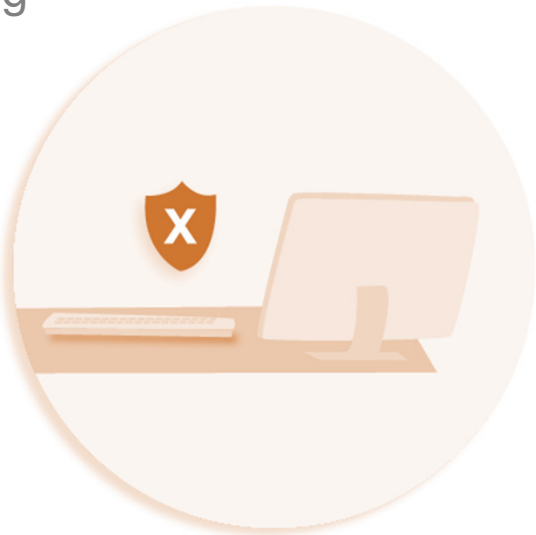
über ihn weiß

DATENSCHUTZ IST GRUNDRECHTSSCHUTZ

- Art. 8 der EU-Grundrechtecharta: „Schutz personenbezogener Daten“
- Recht auf informationelle Selbstbestimmung



Schutz der Person
= Datenschutz



Schutz der Daten
= IT-Sicherheit

Artikel 8 Grundrechts-Charta der EU

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

- Volkszählungsurteil 1983: BVerfG leitet das „**Recht auf informationelle Selbstbestimmung**“ aus den Artikeln 1 und 2 des Grundgesetzes (GG) ab:

  Artikel 1 Abs. 1 GG: „*Die Würde des Menschen ist unantastbar.* […]“

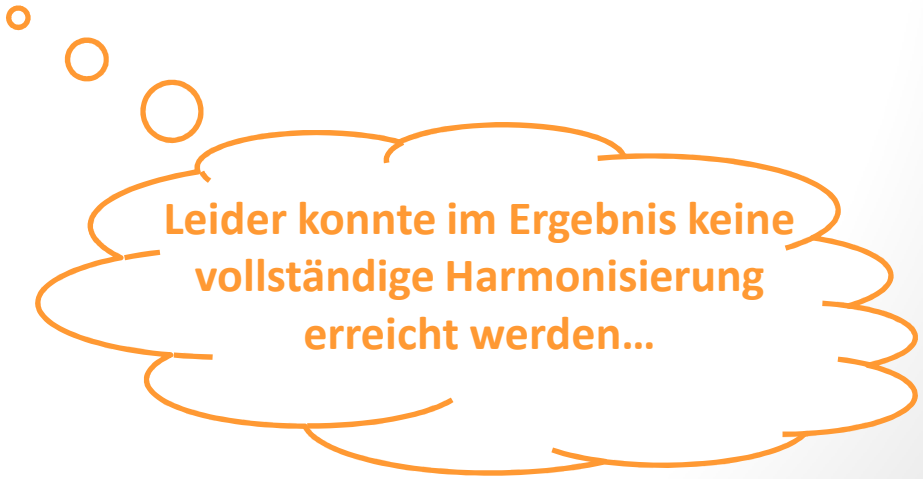
  Artikel 2 Abs. 1 GG: „*Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt* […]“

  - BVerfG „**Recht auf informationelle Selbstbestimmung**“: „Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

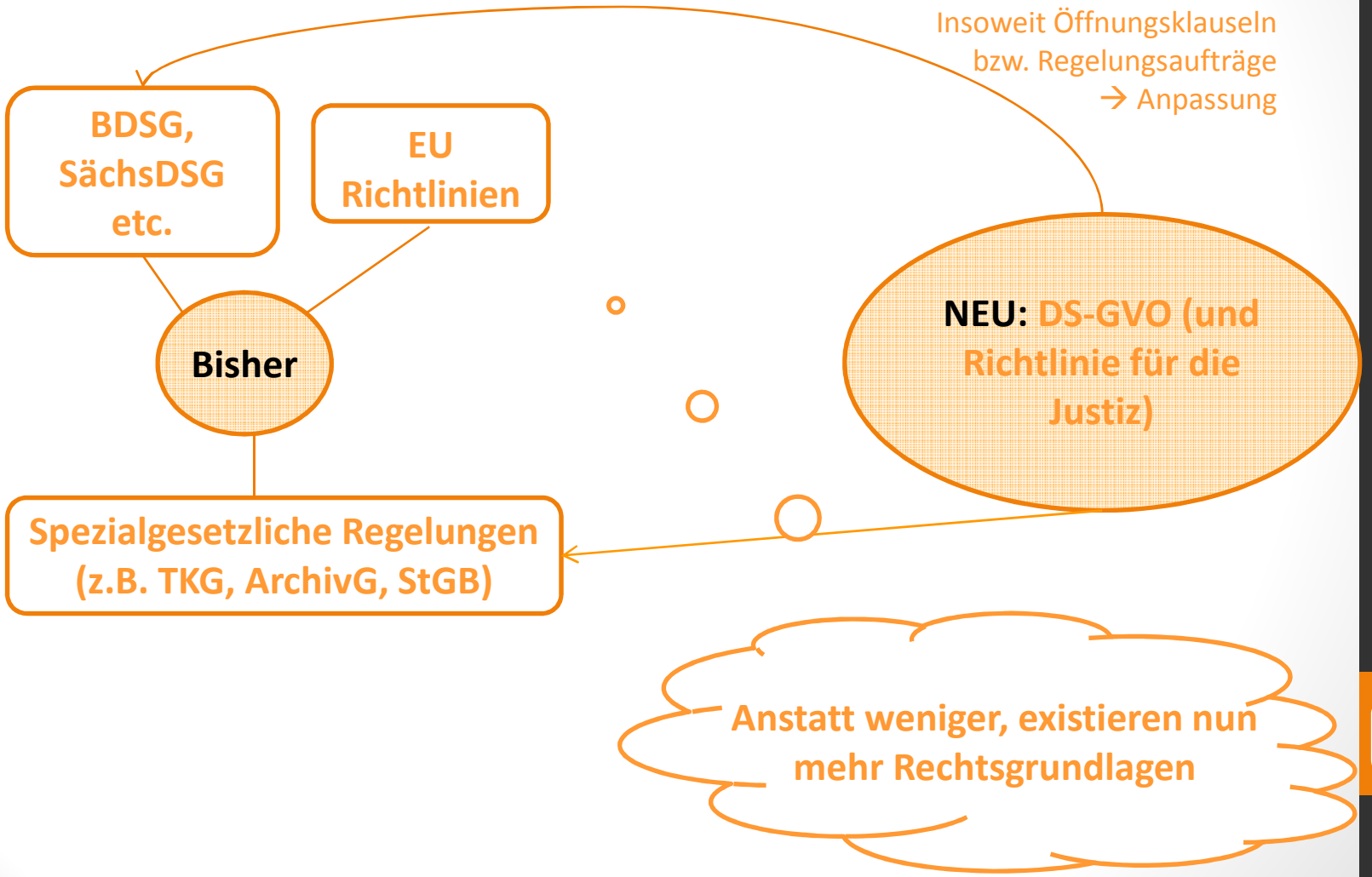
- maßgebend für den Datenschutz sind in Deutschland das Bundesdatenschutzgesetz (BDSG), die Landesdatenschutzgesetze und ab Mai 2018 die Verordnung 2016/679 der EU

d. Datenschutzreform in Europa

- aus dem Ziel einer Verordnung wurde eine Datenschutz-Grundverordnung (DS-GVO)
- zahlreichen Öffnungsklauseln, welche durch die nationalen Gesetzgeber interpretiert und durch nationale Regelungen gefüllt werden können bzw. müssen



Was bedeutet das für den Datenschutz in Deutschland?



Wesentliche Änderungen

1) Deutliche Ausweitung der Dokumentationspflichten (vgl. Art. 5 Abs. 2 DS-GVO)
2) Deutliche Ausweitung der Betroffenenrechte (inkl. Festlegung von Fristen, vgl. Art. 12-23 DS-GVO)
3) Nicht: Deutliche Ausweitung der Bußgeldtatbestände und -höhen
4) Risikobeurteilungen und Folgenabschätzung (in weiterem Umfang, als bisherige Vorabkontrolle)
5) Privacy by design und by default werden verbindlich
6) Mehr Pflichten für Auftragsverarbeiter

Weitere Entwicklung

- Die EU möchte die aktuelle ePrivacy-Richtlinie (Online-Bereich) nun ebenfalls durch eine Verordnung ablösen.
- „Ausfüllungs“gesetze der Mitgliedstaaten.
- Deutschland: Landesgesetze.
- Im Bereich der JI-Richtlinie Umsetzungsgesetze auf Bundes- und Landesebene.
- Änderung des Fachrechts.
- Sonderrecht für nicht „vergemeinschaftete“ Bereiche?
- Verwaltungspraxis.
- EuGH-Entscheidungen.

e. Die Datenschutzgesetze

Struktur der DS-GVO

Kapitel 1: Allgemeine Bestimmungen

Kapitel 2: Grundsätze

Kapitel 3: Rechte der betroffenen Person

Kapitel 4: Verantwortlicher und Auftragsverarbeiter

Kapitel 5: Übermittlung an Drittländer oder an internationale Organisationen

Kapitel 6: Unabhängige Aufsichtsbehörden

Kapitel 7: Zusammenarbeit und Kohärenz

Kapitel 8: Rechtsbehelfe, Haftung und Sanktionen

Kapitel 9: Vorschriften für besondere Verarbeitungssituationen

Kapitel 10: Delegierte Rechtsakte und Durchführungsrechtsakte

Kapitel 11: Schlussbestimmungen

Struktur des BDSG (neu)

Teil 1: Gemeinsame Bestimmungen

Teil 2: Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Art. 2 der DS-GVO

Teil 3: Bestimmungen für Verarbeitungen zu Zwecken gemäß Art. 1 Abs. 1 der DSRL

Teil 4: Besondere Bestimmungen für Verarbeitungen im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich der DS-GVO bzw. der DSRL fallen

f. Anwendungsbereich des Datenschutzes

- Der Anwendungsbereich wird auf alle Verarbeitungen personenbezogener Daten ausgeweitet, die sich an Personen in der EU richten und deren personenbezogene Daten verarbeiten (sog. Marktortprinzip)

Bsp.: Türkisches Unternehmen bietet EU-Bürgern Waren im Online-Shop an.

Auch „unentgeltliche“ Internetangebote wie Suchdienste und soziale Netzwerke sind erfasst.

Personenbezogene Daten

…sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DS-GVO) – Beispiele:

Foto

Vermögensverhältnisse

Kennzeichen

Wohnverhältnisse

Bankdaten

Körpergröße

Personalnummer

Adresse

Name

Hobby

Telefonnummer

Geburtstag

IDENTIFIZIERT ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

IDENTIFIZIERBAR wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Information feststellbar wird.

„Besondere Kategorien personenbezogener Daten“ (sensible Daten) - Art. 9 DS-GVO

Rassische und ethnische Herkunft

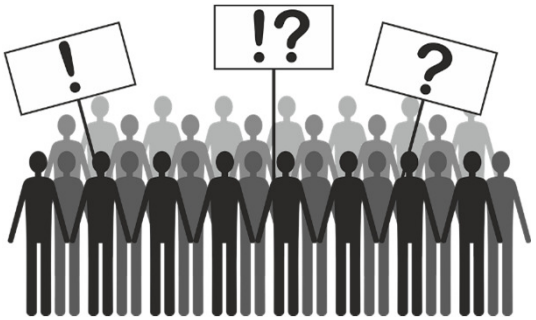
Religiöse oder weltanschauliche Überzeugungen

Gesundheit

Neu: Genetische Daten

Sexualleben/ sexuelle Orientierung

Gewerkschaftszugehörigkeit

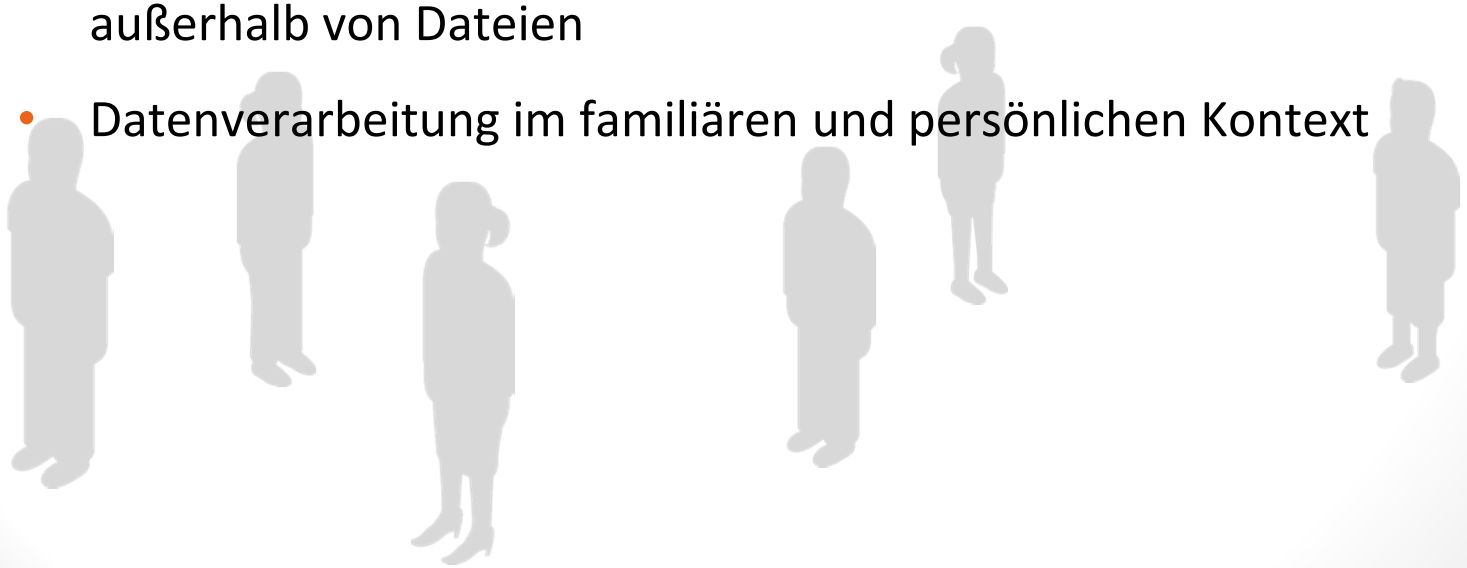


Neu: Biometrische Daten

Politische Meinungen

Vom Datenschutz nicht geschützt werden:

- Daten von juristischen Personen, Vereinen, Verbänden etc.
- Daten von Toten
- Daten ohne Personenbezug (anonyme Daten, u.U. Betriebs- und Unternehmensgeheimnisse)
- teils Daten außerhalb automatisierter Verarbeitung und außerhalb von Dateien
- Datenverarbeitung im familiären und persönlichen Kontext



Anonymisieren & Pseudonymisieren

Anonymisieren

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

Fließende Übergänge

Ziel: Ausschluss oder Erschwerung der Bestimmbarkeit der – hinter einem Datum stehenden - Person und damit Wegfall des Personenbezugs

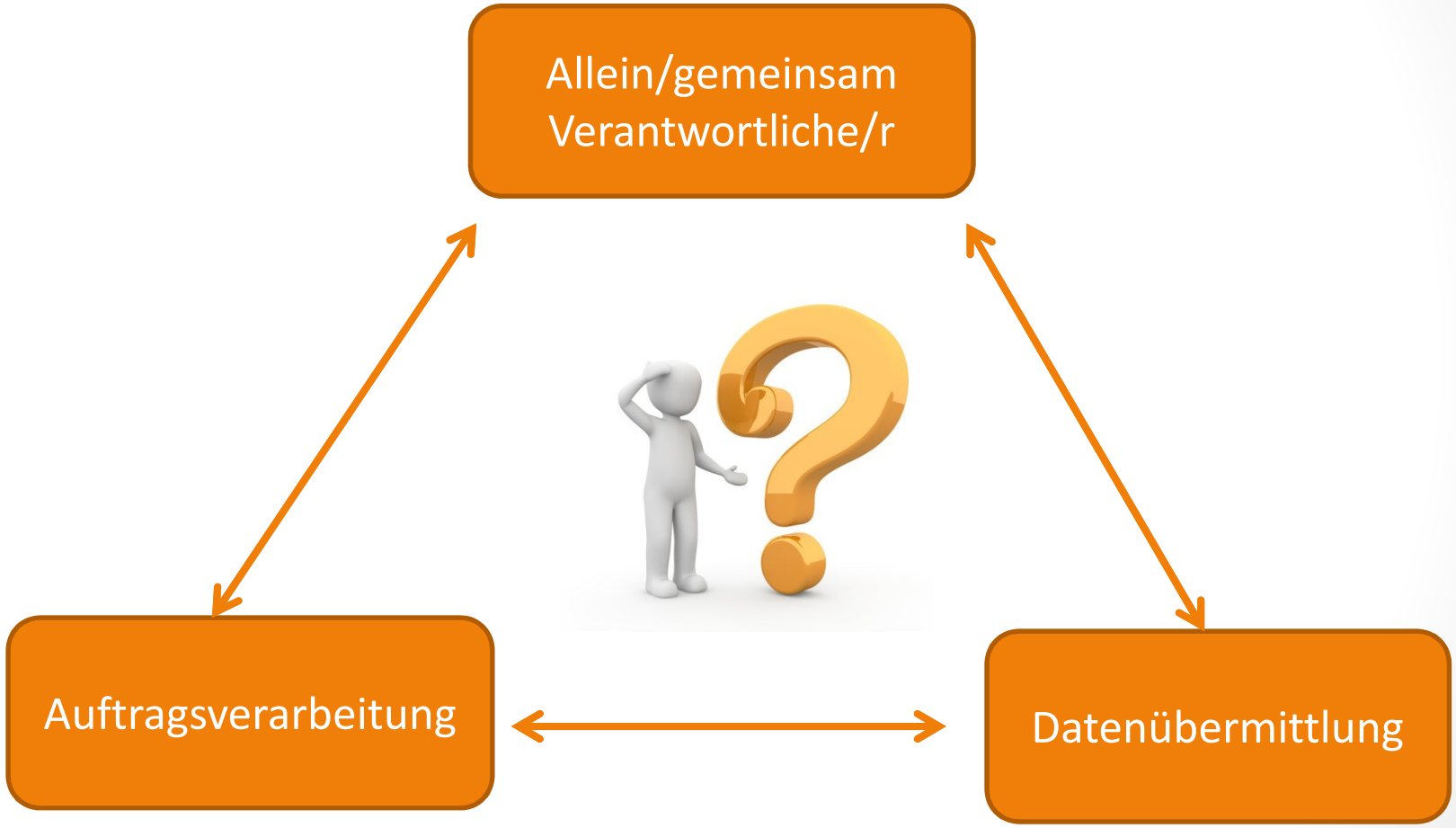
Pseudonymisieren

… ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.


Ihr Google-Herzschrittmacher hat uns benachrichtigt, dass wir hier gleich gebraucht werden
GDD forever!
GRESER&LENZ

Internet 4.0

2. Beteiligte Personen

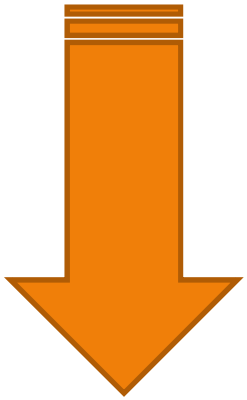


- **Betroffene Person im Sinne des Art. 4 Nr. 1 DS-GVO ist diejenige natürliche Person, deren Daten verarbeitet werden.**
- Den betroffenen Personen werden Rechte eingeräumt.

(eine Seite der Medaille)

Verantwortliche Stelle / Verantwortlicher

[…] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet[…] (Art. 4 Nr. 7 DS-GVO)



GmbH/AG, OHG, Einzelunternehmer, Behörde, niedergelassener Arzt…

Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. ***Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt****, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt,[…]. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.*

→ muss die jeweiligen **tatsächlichen Funktionen und Beziehungen** der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln

→ Das wesentliche der Vereinbarung wird der **betroffenen Person zur Verfügung gestellt**.

→ Ungeachtet der Einzelheiten der Vereinbarung kann die betroffene Person ihre Rechte **bei und gegenüber jedem einzelnen der Verantwortlichen** geltend machen.

Gemeinsame Datenverarbeitung (Joint Controllership)

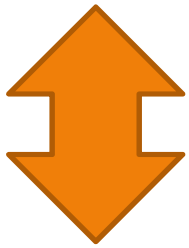
- Zwei verantwortliche Stellen verarbeiten gemeinsam Daten mit jeweils vertraglich festgelegten Verantwortlichkeiten
- Art. 4 Nr. 7 DS-GVO: arbeitsteiliges Zusammenwirken
- Art. 26 DS-GVO: keine zahlenmäßige Beschränkung

≠ Alleinige verantwortliche Stelle, die die Entscheidungen über Zwecke und Mittel der Verarbeitung selbst und unabhängig von anderen Stellen trifft

≠ Auftragsverarbeitung

Klärung der Verantwortlichkeiten und Zuständigkeiten

Vereinbarung in transparenter Form
(Vereinbarung gemäß
Art. 26 Abs. 1 S. 2 DS-GVO bzw. § 63 BDSG (neu) oder
internes Datenschutzkonzept/Handbuch)



„Zuständigkeit“ (für konkrete Aufgabe)

Auftragsverarbeitung

- Liegt vor, wenn personenbezogene Daten **durch „Dritte“ als Dienstleistung („im Auftrag“) verarbeitet** werden sollen
- Das Gesetz geht davon aus, dass der Auftraggeber gegenüber dem Auftragnehmer eine stärkere Machtposition aufweist und daher bspw. umfassend weisungsberechtigt ist.

Beispiele:

- Vernichtung von vertraulichen Unterlagen im Auftrag
- Ausführung der Lohn- und Gehaltsabrechnung
- Betreuung bzw. Bereitstellung von Netzwerkdiensten
- Cloud Computing
- Wartungsarbeiten an Datenverarbeitungsanlagen
- Call-Center

Auswahl, Vertrag zur Auftrags(daten)verarbeitung und Kontrolle
Vgl. Art. 28 DS-GVO, Erwägungsgrund 81
Achtung: § 62 BDSG (neu) gilt nur für Justiz etc.

KEIN DRITTER, D.H. KEINE ÜBERMITTLUNGSGRUNDLAGE ERFORDERLICH!

- für das Vorliegen einer Auftragsvereinbarung spricht es, wenn

  - dem Auftragsverarbeiter die Entscheidungsbefugnis über die Daten fehlt
  - der Auftragsverarbeiter mit der Datenverarbeitung keine eigenen Geschäftszwecke verfolgt
  - der Auftragsverarbeiter einem ausdrücklichen Nutzungsverbot in Bezug auf die zu verarbeitenden Daten unterliegt
  - der Auftrag auf die Durchführung einer Datenverarbeitung gerichtet ist, die aber nach außen hin dem Verantwortlichen zugerechnet wird
  - der Auftragsverarbeiter im Zusammenhang mit der Auftragsverarbeitung in keinerlei vertraglichen Beziehungen zu den von der Datenverarbeitung Betroffenen steht

Begriffe: Empfänger & Dritter

- Empfänger (Art. 4 Nr. 9 DS-GVO)

> „[…] natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht."

- Dritter (Art. 4 Nr. 10 DS-GVO)

> „[…] natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten."

Begriff „Empfänger“

Agenda 03.05.2018

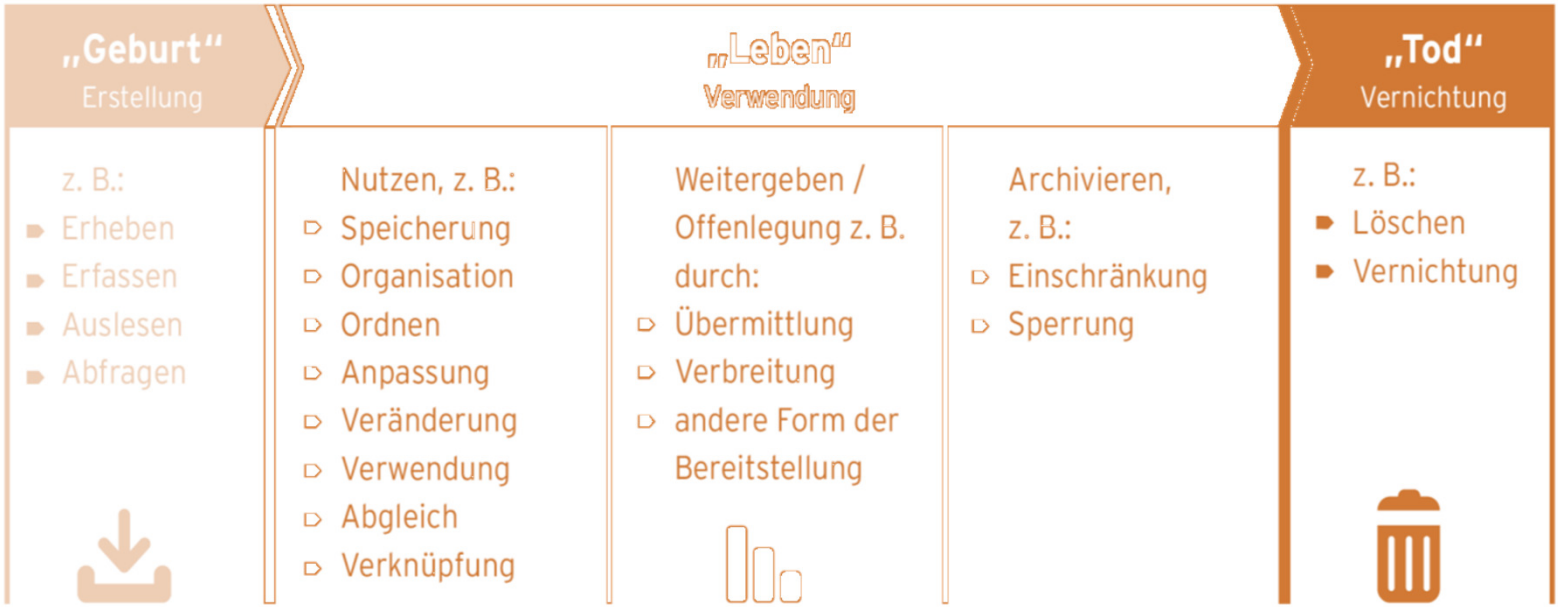
III. Einführung in den Datenschutz und das Datenschutzrecht
   3. Zulässigkeit der Datenverarbeitung
      a. Verbot mit Erlaubnisvorbehalt
      b. Prinzipien der Datenverarbeitung
      c. Verarbeitungstatbestände nach der DS-GVO
      d. Besondere Zulässigkeitsvoraussetzungen
   4. Beschäftigtendatenschutz
      a. Begründung des Beschäftigtenverhältnisses
      b. Durchführung des Beschäftigtenverhältnisses

3. Zulässigkeit der Datenverarbeitung

Begriff: Verarbeiten (Art. 4 Nr. 2 DS-GVO)

- „mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten […]“
- bisherige Dreiteilung (Erheben, Verarbeiten, Nutzen) entfällt
- = Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung oder jede andere Form der Bereitstellung, Abgleich oder Verknüpfung, Löschen oder Vernichtung von personenbezogenen Daten
- automatisierte Verfahren mittels IT-Systemen, Kundenkartei in Dateisystem, Ordnung nach bestimmten Kriterien

Zulässigkeit der Datenverarbeitung



a. Verbot mit Erlaubnisvorbehalt

Die EU-DS-GVO ist als Verbotsgesetz mit Erlaubnisvorbehalt ausgestaltet. Das bedeutet, dass die *Verarbeitung mit personenbezogenen Daten grundsätzlich untersagt* ist, es sei denn die Verordnung, eine andere gesetzliche Vorschrift oder eine Einwilligung des Betroffenen erlauben sie.

Es muss immer geprüft werden, ob eine Verwendung im Einzelfall erlaubt ist.
Hierfür ist der Zweck, für den **die Daten verarbeitet werden sollen, möglichst konkret festzulegen.**

Der Umgang mit personenbezogenen Daten ist zulässig, wenn er…

durch die DS-GVO, BDSG (neu) selbst ...
Beispiel: öffentlich zugängliche Daten, Vertrag

oder durch eine andere Rechtsvorschrift ...
z.B. StGB, SGB, TMG, Betriebsvereinbarung
ABER: Im Einklang mit DS-GVO!

oder durch die Einwilligung des Betroffenen ...
Beispiel: Fotoveröffentlichung, Werbung

... erlaubt wird.

b. Prinzipien der Datenverarbeitung

Zweckbindung

Rechtmäßigkeit
Treu und Glauben
Transparenz

Datenminimierung

Rechenschaftspflicht
(„Accountability“)

Richtigkeit

Speicherbegrenzung

Integrität und
Vertraulichkeit

- Die DS-GVO regelt folgende **sechs Grundsätze** für die Verarbeitung personenbezogener Daten:

(1) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

- die Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn eine Rechtsgrundlage für die Datenverarbeitung vorliegt („Verbot mit Erlaubnisvorbehalt“)
- Transparenz als Teil des Rechts auf informationelle Selbstbestimmung

(2) Zweckbindung (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)

- die Zwecke der Datenverarbeitung müssen bereits bei der Erhebung personenbezogener Daten festgelegt, eindeutig und legitim sein
- eine Weiterverarbeitung zu anderen Zwecken ist nur möglich, sofern die Zwecke der Weiterverarbeitung nicht mit den ursprünglichen Erhebungszwecken unvereinbar sind und eine Rechtsgrundlage für die neue Verarbeitung vorliegt

(3) Datenminimierung

- personenbezogene Daten müssen dem Zweck angemessen und erheblich sein sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden (= Grundsatz der Datenminimierung)

(4) Richtigkeit der Datenverarbeitung

- personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein
- personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, sollen unverzüglich gelöscht oder berichtigt werden

(5) Speicherbegrenzung

- mit der normierten Speicherbegrenzung dürfen personenbezogene Daten nur in einer Form gespeichert werden, die die Identifizierung der Person nur solange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist
- sobald die Speicherung personenbezogener Daten für den Verarbeitungszweck nicht mehr erforderlich ist, müssen die personenbezogenen Daten (mindestens der Personenbezug) gelöscht werden

(6) Integrität und Vertraulichkeit

- personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet
- dies umfasst auch den Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung der personenbezogenen Daten
- hierfür sind geeignete technische und organisatorische Maßnahmen zu treffen

c. Verarbeitungstatbestände nach der DS-GVO

- … die den Umgang mit personenbezogenen Daten erlauben (**Art. 6 DS-GVO**)
  - ✓ Einwilligung
  - ✓ Vertragsabwicklung
  - ✓ Rechtliche Verpflichtung der verantwortlichen Stelle
  - ✓ Lebenswichtige Interessen einer Person
  - ✓ Aufgabenerfüllung im öffentlichen Interesse
  - ✓ Bei Privaten: berechtigtes Interesse nach Abwägung
- für besondere Datenkategorien (sensitive Daten) gelten die höheren Anforderungen der Art. 9 und 10 DS-GVO

Die Einwilligung

… „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“ (Art. 4 Nr. 11 DS-GVO)

- Freiwilligkeit
  Kein Ungleichgewicht
- Aktive Handlung
- Verständlich, leicht zugängliche Form, klare und einfache Sprache, Hervorhebung
- Keine Nachteile
- Konkreter Zweck, Erforderlichkeit
- Nachweis der Einwilligung
- Information, vgl. Art. 13 DS-GVO
- Jederzeitiges Widerrufsrecht
- Einhaltung der DS-GVO

- Der Betroffene ist über folgende Punkte ***vor*** der Erteilung seiner Einwilligung zu unterrichten:
  - ✓ Identität der verantwortlichen Stelle
  - ✓ Benennung der Art der zu verarbeitenden Daten (Datenkategorien)
  - ✓ Zweck der Datenverarbeitung
  - ✓ Umfang und Form der Verarbeitung
  - ✓ Aufklärung über mögliche Verknüpfungen mit anderen Datenbeständen
  - ✓ Bei einer beabsichtigten Datenübermittlung: auch der künftige Datenempfänger
  - ✓ Bei Daten gem. § 3 Abs. 9 BDSG (alt) (besonders sensible Daten) die ausdrückliche Benennung der betroffenen Daten
  - ✓ Hinweis auf die Möglichkeit der Verweigerung oder des Widerrufs mit Wirkung für die Zukunft.
  - ✓ Aufklärung über die Rechtsfolgen, wenn er die Einwilligung erteilt
  - ✓ Aufklärung über die Rechtsfolgen, wenn er die Einwilligung nicht erteilt

Achtung bei:

- Einwilligungen in AGB bzw. gemeinsam mit anderen Informationen
- Einwilligung von Kindern
- Einwilligung bzgl. sensibler Daten (z.B. Gesundheit, Gewerkschaftszugehörigkeit)
- Einwilligung im Arbeitsverhältnis

Im Falle einer unwirksamen Einwilligung
ist die Datenverarbeitung u.U. unzulässig!

Neu: Kopplungsverbot

„[…]Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.“ (Erwägungsgrund 43)

Das Kopplungsverbot galt bisher nur für Leistungen, die nicht anderweitig in Anspruch genommen werden konnten, z.B. aufgrund der Marktmacht oder kein Wettbewerb

<u>Beispiel:</u>

Einwilligung in Übermittlung der Adressdaten an Werbepartner z.B. im Rahmen eines Gewinnspiels bzw. eines Vertrages

Muster Einwilligungserklärung

- in die Veröffentlichung von Fotos durch die * -**

Die *** beabsichtigt, für Zwecke der Werbung, Außendarstellung und zur Information der Öffentlichkeit über das Unternehmen und seiner Mitarbeiter Fotos zu veröffentlichen. Hierbei handelt es sich aktuell insbesondere um Profilbilder der einzelnen Mitarbeiter sowie zukünftig ggf. auch Gruppen- bzw. Aktionsbilder. Eine darüber hinausgehende Nutzung der Fotos oder der Veröffentlichung in weiteren Medien bedarf einer gesonderten Einwilligung. Ton-, Video-, Webcam- und Filmaufnahmen sind von der Einwilligung nicht umfasst.

Zu diesem Zweck erkläre ich mich mit der Veröffentlichung meiner Fotos

- ☐ **im Intranet der *****
- ☐ **im Internet**
- ☐ **in Printmedien (z.B. in Anzeigen, Broschüren, Präsentationen, Flyern, Plakaten)**

einverstanden. (Bitte zutreffendes ankreuzen.)

Durch eine Veröffentlichung im Internet kann weltweit von jedermann auf die Fotos zugegriffen werden. Es ist möglich, dass Dritte die veröffentlichten Bilder herunterladen und für nicht bekannte Zwecke auch nach einem Widerruf dieser Einwilligung nutzen. Über die Archivfunktion von Suchmaschinen besteht die Möglichkeit, dass Daten auch dann noch abrufbar sind, wenn die Angaben aus den Internetangeboten der *** bereits entfernt oder geändert wurden.

Die Erteilung der Einwilligung ist **freiwillig**. Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft schriftlich widerrufen werden. Aus der Verweigerung der Einwilligung oder ihrem Widerruf entstehen keine Nachteile. Im Falle eines Widerrufs werden meine Fotos entfernt bzw. gelöscht.

Bei Veröffentlichung von Gruppenfotos führt der spätere Widerruf einer einzelnen Person grundsätzlich nicht zu einem nachträglichen Entfernen des Bildes, es sei denn, dass die Interessen des betroffenen Mitarbeiters im Einzelfall überwiegen.

Die Einwilligung endet nicht automatisch mit dem Ausscheiden aus der ***. Im Falle eines Widerrufs werden meine Fotos entfernt bzw. gelöscht. Dies kann bis zu 3 Werktage in Anspruch nehmen.

_____ _____

Ort, Datum Unterschrift des Mitarbeiters

Vertrag

„die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen“ (Art. 6 Abs. 1 lit. b DS-GVO)

Problem: Was ist erforderlich?

Beispiele:

- Adressdaten für Versand
- Angebotsanfrage unter Nennung der Kontaktdaten
- Informationen über die eigene Person im Rahmen der Rechtberatung

Zweckänderung

… zulässig bei Vereinbarkeit mit ursprünglichen Zweck der Datenerhebung

Oder:
Einwilligung
Rechtsvorschrift

Art. 6 Abs. 4 DS-GVO, Erwägungsgrund 50:
Kriterien zur Kompatibilitätsprüfung (nicht abschließend)

Information des Betroffenen!
Betroffenenrechte!

Weitere Rechtmäßigkeitsgrundlagen

- Rechtliche Verpflichtung
- Schutz lebenswichtiger Interessen
- Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde
- Berechtigte Interessen des Verantwortlichen oder eines Dritten und keine überwiegenden entgegenstehenden Interessen
- Ggf. spezifische nationale Rechtsgrundlagen
- Verarbeitung von Daten über strafrechtliche Verurteilungen & Straftaten nur nach Art. 10 DS-GVO

d. Besondere Zulässigkeitsvoraussetzungen

Besondere Arten personenbezogener Daten

Art. 9 DS-GVO: Verarbeitung ist untersagt - Ausnahmen:

a) **Ausdrückliche Einwilligung**, insoweit dies nicht spezialgesetzlich ausgeschlossen ist

b) **Rechte und Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes im Rahmen spezialgesetzlicher Regelungen oder Kollektivvereinbarungen**

c) Lebenswichtige Interessen, aber betroffene Person kann aus körperlichen oder rechtlichen Gründen keine Einwilligung geben

d) Organisationen ohne Gewinnerzielungsabsicht

e) Durch die betroffene Person veröffentlichte Daten

f) **Rechtsansprüche**

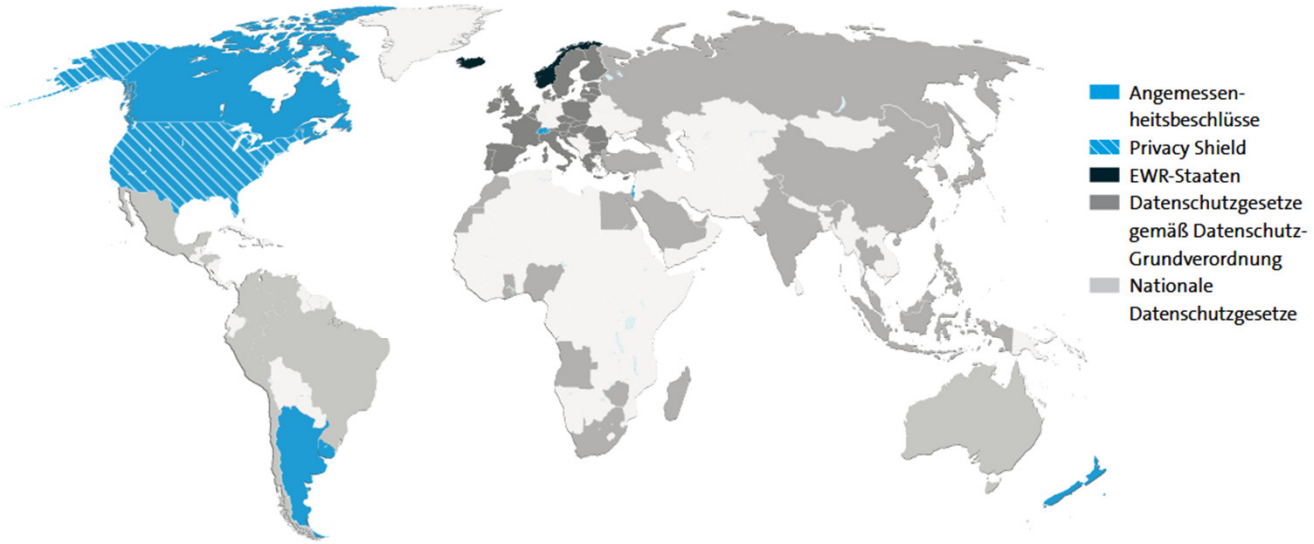
g) Auf Grundlage spezialgesetzl. Regelung erhebliches öffentliches Interesse

h) Auf Grundlage spezialgesetzlicher Regelung für Gesundheitsvorsorge, Arbeitsmedizin, Gesundheits- und Sozialbereich etc.

i) Öffentliches Interesse im Bereich der öffentlichen Gesundheit

j) Auf Grundlage spezialgesetzlicher Regelung für im öffentlichen Interesse liegende Archivzwecke, Forschungszwecke oder statistische Zwecke

Datenverarbeitung in einem Drittland mit angemessenem Datenschutzniveau



Hinweis: Laut EU-Kommission haben in den vergangenen Jahren weltweit immer mehr Länder neue Datenschutzvorschriften erlassen oder einen entsprechenden Prozess in Gang gesetzt. 2015 verfügten laut EU-Kommission insgesamt 109 Länder über Datenschutzgesetze, ein erheblicher Anstieg gegenüber den 76 Ländern, die Mitte 2011 gezählt wurden, ↗EU-Mitteilung (2017) 7, p. 8. In 2017 ist diese Zahl nochmal um 10 % auf 120 Länder angestiegen.

Quelle: Greenleaf, Graham; Global data privacy law (5th edition 2017) Stand Juni 2017

Datenverarbeitung in Drittstaaten ohne angemessenes Datenschutzniveau

Gesetzliche Ausnahmetatbestände (Art. 49 DS-GVO)

Zur Vertragsverfüllung notwendige Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau

- ausnahmsweise zulässig, wenn zwischen dem Betroffenen und Verantwortlichen ein Vertrag abgeschlossen worden ist, für dessen Erfüllung die Datenübermittlung erforderlich ist
- gilt auch, wenn Übermittlung zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist

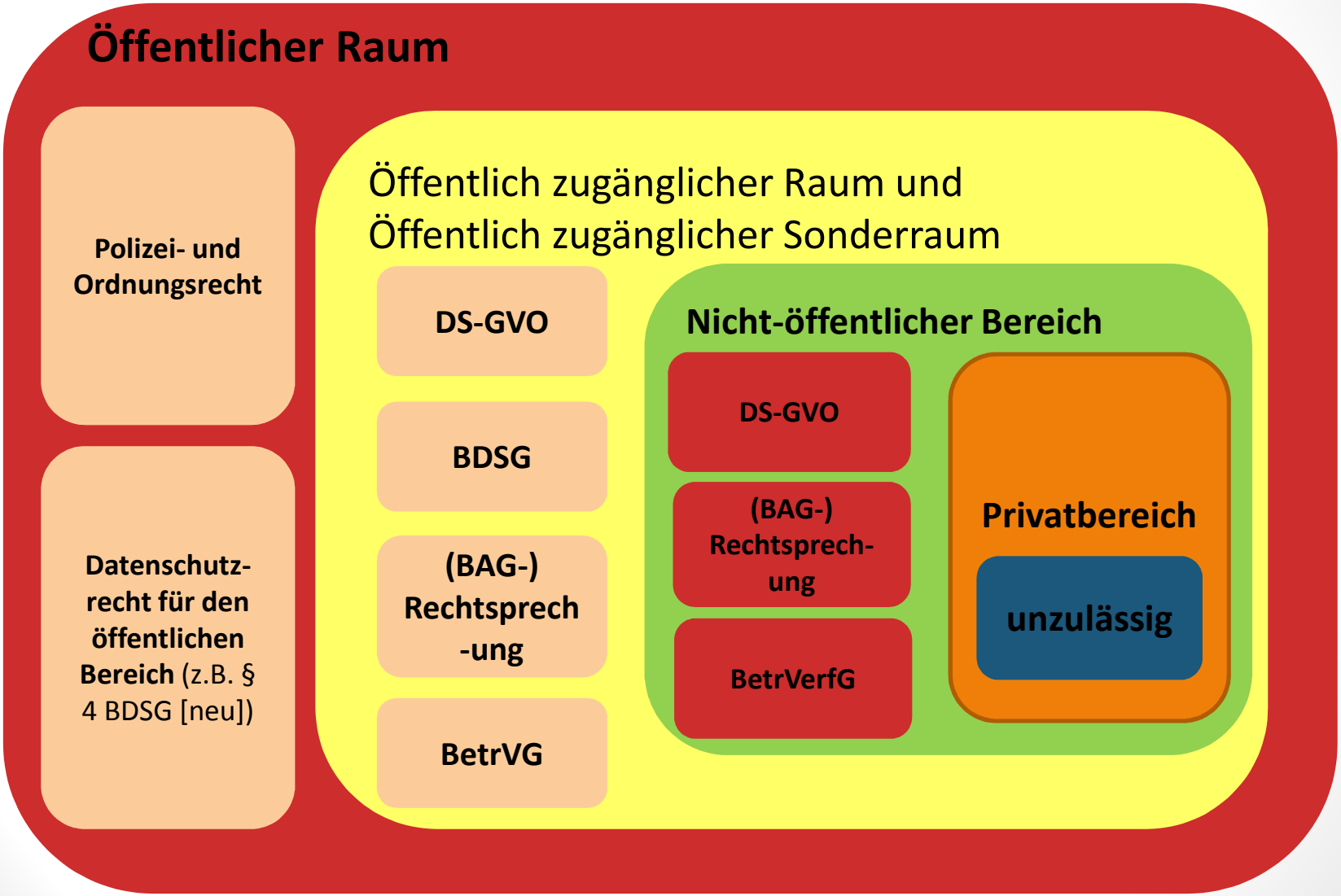
Beispiel: Kunde (K) möchte, dass sein Reisebüro für ihn in Peking ein Hotelzimmer reserviert. Das Reisebüro kann sich für die Übermittlung der Daten des (K) an das Hotel in Peking auf Art. 49 Abs. 1 S. 1 lit. b DS-GVO berufen, da zur Durchführung bzw. Erfüllung des Vertrages zwischen (K) und dem Reisebüro die Weitergabe seiner Daten zwingend notwendig ist.

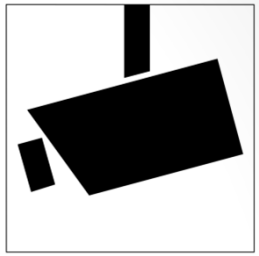
Geeignete Garantien

- geeignete Garantien können für Schutz der Betroffenen den im Drittland bestehenden Mangel an Datenschutz ausgleichen

Garantien ohne besondere Genehmigung der Aufsichtsbehörden	Garantien, die dem Vorbehalt der Genehmigung der zuständigen Aufsichtsbehörden unterliegen
• rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen • verbindliche interne Datenschutzvorschriften (BCR) gemäß Art. 47 DS-GVO • Standarddatenschutzklauseln, die von der Kommission (gem. Prüfverfahren nach Art. 93 Abs. 2) erlassen wurden • von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln, die von der Kommission geprüft und genehmigt wurden • genehmigte Verhaltensregeln gem. Art. 40 • genehmigte Zertifizierungsmechanismen gem. Art. 42	• Vertragsklauseln, die zwischen Verantwortlichen und Auftragsverarbeiter oder Empfänger der personenbezogenen Daten im Drittland vereinbart wurden • Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden und öffentlichen Stellen aufzunehmen sind

Videoüberwachung





- **Beobachtung** öffentlich zugänglicher Räume
- **Zulässigkeit** der Videoüberwachung
  - Aufgabenerfüllung öffentlicher Stellen
  - Wahrnehmung des Hausrechts
  - Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

  und kein Entgegenstehen überwiegender schutzwürdiger Interessen der Betroffen
- **Erkennbarkeit** der Maßnahme und Kontaktdaten des Verantwortlichen
- **Speicherung oder Verwendung** der Daten nur bei Erforderlichkeit
- werden Videodaten einer bestimmten Person zugeordnet, besteht Informationspflicht
- **Löschungsverpflichtung**
  - bei Zweckerfüllung
  - Entgegenstehen schutzwürdiger Interessen der Betroffenen

- **Was sind öffentlich zugängliche Räume?**
  - Bereiche, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach dazu auch bestimmt sind
  - Eigentumsverhältnisse irrelevant
  - ebenso irrelevant, ob der Ort umschlossen oder überdacht ist oder eine Zugangs- bzw. Nutzungsberechtigung z.B. in Form eines Tickets erworben werden muss
  - umfasst die Anwendung von Videoeinsätzen auf Parkplätzen, an Haltestellen und Tankstellen, auf öffentlichen Gehwegen und Straßen, in Parks, Fußgängerzonen, Ladengalerien, Geschäften, Bibliotheken, Bahnhöfen, öffentlichen Verkehrsmitteln, Fußballstadien, Museen, Banken, Spielhallen, auch in gemischt genutzten Wohn- und Geschäftshäusern - begrenzt auf die Öffnungszeiten bzw. Sprechstunden

- Ebenfalls erfasst sind Eingangsbereiche vor der Haustür, sofern sie sich auf bzw. an einem öffentlich zugänglichen Weg und nicht innerhalb einer abgegrenzten Anlage befinden.

- **Keine** öffentlich zugänglichen Räume i.S.d. § 4 Abs. 1 BDSG (neu) sind grundsätzlich Wohnungen, Hausflure, geschlossene Wohnanlagen, Vorgärten, Firmengelände, Büros, Werkhallen, Lager- und Personalräume oder sonstige interne, besonders geschützte, nicht für Publikumsverkehr vorgesehene Bereiche.

Kennzeichnung der Videoüberwachung

Insgesamt lässt sich die Videoüberwachung **datenschutzrechtlich** wie folgt bewerten:

- Jede Videoüberwachung ist ein Eingriff in das Persönlichkeitsrecht, denn alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.
- Die Videoüberwachung erfasst unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen.
- Daher ist Videoüberwachung immer begründungsbedürftig und darf nur offen erfolgen, sie ist stets auf das notwendige Maß zu beschränken und bedarf in zeitlicher Hinsicht der regelmäßigen Überprüfung (jährliche Evaluationspflichten).
- Vor der Einrichtung einer Videoüberwachung müssen alle Alternativen hierzu geprüft und bewertet werden.
- Videoüberwachung kann nur ultima ratio sein.

5. Beschäftigtendatenschutz

Zentrale Regelung: § 26 BDSG (neu)

bisher: § 32 BDSG - Neu: in DSGVO keine Regelung, sondern umfangreiche Öffnungsklausel - § 26 BDSG (neu):

„Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.“ (Abs. 1)

Wer zu dem Kreis der Beschäftigten im Rahmen des Datenschutzrechts gehört, findet sich in § 26 Abs. 8 BDSG (neu)

„Beschäftigte“

- **Arbeitnehmerinnen und Arbeitnehmer**, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
- zu ihrer **Berufsbildung** Beschäftigte,
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (**Rehabilitandinnen und Rehabilitanden**),
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- **Freiwillige**, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
- Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als **arbeitnehmerähnliche Personen** anzusehen sind; zu diesen gehören auch die in **Heimarbeit** Beschäftigten und die ihnen Gleichgestellten,
- Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende,
- **Bewerberinnen und Bewerber** für ein Beschäftigungsverhältnis sowie **Personen, deren Beschäftigungsverhältnis beendet** ist,

gelten als Beschäftigte.

Personenbezogene Daten im Beschäftigtendatenschutz

Alle Daten, die sich auf einen Beschäftigten beziehen oder dessen Person oder die beruflichen oder sonstigen Lebensumstände beschreiben, z.B.:

- Stammdaten, Schul- und Berufsausbildung, Berufserfahrung, Familienverhältnisse), Personalaktendaten, Vertrags-, Gehalts- und Lohnabrechnungsdaten, Beurteilungen, Zielvereinbarungen, Urlaubs- und Krankheitszeiten etc.
- Schlüsselzahlen wie Lohn- und Vergütungsgruppe, Personalnummer, Benutzerkennung für die IT-Systeme und alle Daten, die damit verknüpft sind, z.B. Protokolleinträge in DV-Systemen
- Daten ohne unmittelbaren Personenbezug, wenn die Benutzer der Daten anhand von Ordnungsbegriffen oder sonstigen Ordnungskriterien oder anhand von vorhandenem oder ihnen zugänglichem Zusatzwissen die Beschäftigten identifizieren können

Beschäftigtendaten werden unabhängig von ihrer Form geschützt, d.h. es kommt nicht auf eine automatisierte Verarbeitung bzw. Verwendung in oder aus nicht automatisierten Dateien an.

a. Begründung des Beschäftigungsverhältnisses

"I've given you my email, IM, blog, Twitter, Facebook, and LinkedIn profiles and now you want to TALK to me?!"

"OK -- note down this Skype ID..."

Datenschutz im Bewerbungsverfahren

- Eine Datenerhebung ist zulässig, soweit die Daten zur **Entscheidung über die Bewerbung erforderlich** sind (§ 26 Abs. 1 Satz 1 BDSG)
- Datenerhebung: **Trennung nach Bewerbungsverfahren und Einstellung** (Familienstand, Krankenversicherung, Religionszugehörigkeit röm.-kath.. oder evang., Staatsangehörigkeit dürfen z.B. erst nach der Einstellung erfragt werden)
  - **Nur die für die Bewerberauswahl erforderlichen Daten erheben!**
  - bei Bewerberfragebogen: Mitbestimmung gem. § § 94, 95 BetrVG
- für die Einholung von Auskünften und Referenzen i.d.R. Einwilligung erforderlich

- **Entscheidung, ob der Betroffene eingestellt wird**, vgl. Rechtsprechung der Arbeitsgerichte zum Fragerecht

  - **Behinderung:** Jeder Beschäftige entscheidet frei, ob er eine Behinderung mitteilt.

  - **letztes Einkommen bei früherem Beschäftigungsverhältnis**: Die Verwendung ist für die Durchführung eines aktuellen Beschäftigungsverhältnisses nicht erforderlich. (str.)

  - **Vermögensverhältnisse/Schulden**: Eine Verwendung für die Durchführung eines Beschäftigungsverhältnisses ist nicht erforderlich und daher unzulässig. (Ausnahme: Lohnpfändung von Gläubigern)

Aufbewahrung und Rückgabe der Bewerbungsunterlagen

- **Löschung**, sobald die Daten für die Erfüllung des Erhebungszwecks nicht mehr erforderlich sind (Art. 5 DSGVO), aber AGG-Frist (2 Monate zzgl. 1 Monat) beachten, Zurückbehalten der Bewerbung für eine spätere Stelle oder Weiterleitung im Unternehmen nur mit Einwilligung

- **Rückgabe** nur bei Ausschreibung der Stelle nötig, nicht bei Initiativbewerbung

b. Durchführung des Beschäftigungsverhältnisses

- **Erhebung und Nutzung zur Ausführung des Anstellungsvertrags**
- Stamm- und Vertragsdaten, Arbeitszeit, Lohn-, Gehalts- und Abrechnungsdaten, Sozialdaten etc.
- Daten über Anwesenheit, Arbeit, Fehlzeiten und Fehlzeitengründe (keine Krankheitsdiagnosen), Zugangskontrolle
- Foto, z.B. für Werksausweis (Zutrittskontrolle)
- Besondere Datenarten, aber nur bei gesetzlicher Verpflichtung oder bei besonderen Unternehmungen (z.B. kirchlichen Einrichtungen)
- Daten zur Überwachung/Erfassung der vereinbarten Arbeitsleistung, z.B. bei Akkordentlohnung, Zielvereinbarungen

Eine Erhebung ist zulässig, soweit die Daten **für den künftigen Verlauf des Beschäftigungsverhältnisses** von Bedeutung sein können.

- Nutzung, soweit für die Durchführung des Beschäftigungs-verhältnisses erforderlich **(Interessenabwägung)**
- Überwachungs- und Sicherheitssysteme, soweit z.B. aus Sicherheitsgründen oder zur Diebstahlüberwachung etc. erforderlich (Videoüberwachung für festgelegte Zwecke, Zutrittskontrolle)
- Controlling, i. d. R. auf Teamebene (≥ drei bis vier Personen)
- Protokollierung zur Sicherstellung der Verfügbarkeit und Kontrolle der IT-Systeme und zur Kontrolle unzulässiger Nutzungen
- Protokollierung und Protokollauswertungen (private Nutzung der IT- und Kommunikationssysteme und Telekommunikations-geheimnis beachten)

Keine verdeckten und heimlichen Überwachungen, kein übermäßiger Überwachungsdruck, schutzwürdiges Interesse der Betroffenen und Mitbestimmung gem. §§ 87 ff. BetrVG beachten

Erhebung und Nutzung zur Aufdeckung von Straftaten

- Es müssen **tatsächliche Anhaltspunkte** für die Begründung eines Verdachts vorliegen. → **Dokumentation!**
- Es muss sich um eine **Straftat** handeln (Ordnungswidrigkeit reicht nicht aus).
- Es muss sich um eine Straftat **im Beschäftigungsverhältnis** handeln.

  → **Verhältnismäßigkeit!**
- Art und Ausmaß der Verarbeitung dürfen im Hinblick auf den Anlass nicht unverhältnismäßig sein. Das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung darf nicht überwiegen.

BAG Urteil v. 29.06.2017, 2 AZR 597/16: § 32 I 2 BDSG sperrt nicht die verdeckte Überwachung bei Verdacht schwerer Pflichtverletzungen.

Kontrolle der Internet- und E-Mail-Nutzung

- Protokolldateien dürfen u.U. für Auswertezwecke vorgehalten werden (Grundsatz: so lange erforderlich - Dauer max. 1 Jahr?)
- Eine inhaltliche Kontrolle von E-Mails ist nicht zulässig. Ausnahmen:
  - Straftaten
  - schwere Vertragsverletzungen
  - unerlaubte private Nutzung
  - dienstlicher Notwendigkeit (Bsp.: Fristenkontrolle)
- Der Arbeitgeber hat Anspruch auf Herausgabe aller dienstlichen E-Mails.
- Der Arbeitnehmer/Beschäftigte ist Berechtigter an allen (erlaubten) privaten Mails und an „Mischbeständen“.

Nutzung von Kommunikationseinrichtungen

- Entscheidung über die Zulässigkeit der privaten Nutzung von Kommunikationseinrichtungen (Telefon, E-Mail, Internet)
- Erlaubte oder geduldete private Nutzung
  - Auch eine stillschweigende Duldung wird als Erlaubnis der privaten Nutzung ausgelegt
  - Bei einer **erlaubten oder geduldeten privaten Nutzung** fallen die privaten Kommunikationsvorgänge (Inhalt und Protokolldaten) für die Dauer des Übertragungsvorgangs unter den **Schutz des Telekommunikationsgeheimnisses**
- Verbotene private Nutzung

  Bei **Verbot der privaten Nutzung** sind **weitergehende Überwachungsmaßnahmen** im berechtigten Interesse des Arbeitgebers unter Berücksichtigung des schutzwürdigen Interesses der Beschäftigten zulässig.

Kontrolle des E-Mail-Verkehrs

Möglichst anonymisierte Kontrollen (Verkehrsdaten)

- Volumen, Dateiformate, riskante Anhänge (Viren, Trojaner etc.) dürfen kontrolliert werden. (str. für erlaubte Privatnutzung)
- Schädliche Software (Viren etc.) darf gelöscht werden (Nachricht an Adressaten). (wie soeben)
- Prüfung von verschlüsselten Sendungen durch https-Scanning ist in einer Blackbox zulässig, wenn diese eine Kenntnisnahme der Inhalte durch Administratoren ausschließt, wenn ein konkretes Gefährdungspotenzial besteht und die Prüfung zur Gefahrenabwehr erforderlich ist.

Spam

- Spam ist grundsätzlich rechtswidrig
- Filterung, Löschung, Sperrung bestimmter URLs grundsätzlich erlaubt.

Problem:

- False-Positive-Rate
- Kaufmännisches Bestätigungsschreiben
- Bei einer erlaubten privaten Nutzung fällt erwünschter Spam unter den Schutz des Telekommunikationsgeheimnisses

- Löschung von Sendungen mit Schadsoftware ist zulässig. Insbesondere bei einer erlaubten privaten Nutzung Betroffene über die Löschung unterrichten.

Verfahren:

- Spam filtern, schädlichen und rechtswidrigen Spam löschen, nach Möglichkeit den Empfänger unterrichten und den Rest in einem Spamordner zur Verfügung stellen.

Ausscheiden eines Mitarbeiters

- Private E-Mails durch den Arbeitnehmer löschen lassen (Löschung bestätigen lassen)
- Eingehende E-Mails nach dem Ausscheiden:
  - Abwesenheitsnachricht (Adressat nicht mehr zu erreichen)
  - E-Mail-Account nach einer festgelegten oder mit dem Betroffenen zu vereinbarenden Frist löschen

Problem:

Private Daten in Archivsystemen - Regelung mit Einführung des Archivsystems durch Betriebsvereinbarung und ggf. Einwilligung der Betroffenen

Urlaub, Krankheit

- Abwesenheitsnachricht, ggf. mit Verweis auf den Stellvertreter
- Weiterleitung an Vertreter nur mit Einwilligung
- Einsicht in den PC bei Abwesenheit
  - Optimal: schriftliche Benennung einer Person des Vertrauens, die Einsicht nehmen darf. Bei erlaubter privater Nutzung möglichst Einwilligung einholen.
  - Minimallösung: z.B. wenn der Betroffene nicht erreichbar oder nicht ansprechbar ist. Gezielte Suche nach einem bestimmten Dokument (Vier-Augen-Prinzip empfohlen) wird noch für zulässig gehalten (Recht des AG auf Zugriff auf die Geschäftskorrespondenz). Passwortrücksetzung!
  - Als privat erkennbare E-Mails dürfen nicht geöffnet werden.

Personalakte

- Arbeitgeber ist - abgesehen von steuer- und sozialversicherungs-rechtlichen Vorschriften - nicht zur Führung von Personalakten verpflichtet
- Nur Daten, die für die Durchführung des Arbeitsverhältnisses erforderlich sind
- Keine Parallelakten, aber ggf. Teilakten (Aufgliederung nach sachlichen Gründen) zur Trennung von Zuständigkeiten
- Vertraulichkeit inner- und außerbetrieblich, Zugriffssicherung
- Einsichtsrecht des Betroffenen uneingeschränkt in alle Bestandteile (§ 34 Abs. 1 BDSG, § 83 BetrVG)
- Getrennte Führung von Gesundheitsunterlagen
- Aufbewahrungsfristen beachten, z.B. bei Abmahnungen

Vertraulichkeit der Personalakte

- Verschlossene Verwahrung der Personalakten
- Kontrollierter Zugriff auf Personalakten, auch im Vertretungsfall
- Kontrollierter Transport und kontrollierte Weitergabe und Übermittlung
- Grds. Kein Versand von Personaldaten per E-Mail (insoweit erforderlich, nur verschlüsselt)
- Schutz vor unberechtigter Einsichtnahme Dritter
- Einsicht durch BR (-Mitglied) ggf. mit Beschäftigten auf dessen Wunsch hin

Agenda 17.05.2018

III. Einführung in den Datenschutz und das Datenschutzrecht
   4. Beschäftigtendatenschutz
      c. Beendigung des Beschäftigtenverhältnisses
      d. Kollektiver Beschäftigtendatenschutz
   5. Betroffenenrechte
   6. Kundendatenschutz
      a. Zulässigkeit der Kundendatenverarbeitung
      b. Werbeansprachen
      c. „automatisierter Einzelentscheidungen“, Scoring und Profiling

C. Beendigung des Beschäftigungsverhältnisses

- **Speicherung und Nutzung von Daten zur Beendigung**
  - Zulässig sind Vorgänge/Daten über Abmahnung, Kündigung und über die Abwicklung der Beendigung eines Beschäftigungsverhältnisses
  - Zulässig ist die Nutzung vorhandener Daten zur Beendigung eines Beschäftigungsverhältnisses, z.B. zur Sozialauswahl im Zusammenhang mit betriebsbedingten Kündigungen (Mitbestimmung gem. §102 ff. BetrVG beachten)

- **Aufbewahrung und Löschung nach Beendigung**
  - Aufbewahrung/Speicherung von Belegen und Nachweisen lt. gesetzl. Aufbewahrungsfristen (sechs bzw. zehn Jahre)
  - Aufbewahrung im Interesse der Betroffenen (nachvertragliche Fürsorgepflicht), z.B. Zeugnisse, Fortbildungsnachweise, Sozialversicherungsnachweise)
  - Aufbewahrung im Interesse des Unternehmens, z.B. bei Rechtsstreitigkeiten

Löschfristen für Personalakten

- Dauer der Personalaktenführung ist gesetzlich nicht vorgeschrieben
- gilt der allgemeine Grundsatz nach EU-DS-GVO, wonach personenbezogene Daten zu löschen sind, wenn sie für den Zweck der Datenspeicherung nicht mehr erforderlich sind und keine Aufbewahrungsfristen entgegenstehen
  - vor Arbeitsverhältnis
  - während des Arbeitsverhältnisses
  - nach Beendigung des Arbeitsverhältnisses im Abwägungs-prozess (z.B. Ansprüche auf Versorgungsleistungen)

d. Kollektiver Beschäftigtendatenschutz

Bisher: „andere Rechtsvorschriften“
Neu:

[…] durch Kollektivvereinbarungen **spezifischere** Vorschriften zur **Gewährleistung des Schutzes der Rechte und Freiheiten** hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im **Beschäftigungskontext** […]

Art. 88 Abs.1 DS-GVO i.V.m. EG 155, § 26 Abs. 4 BDSG (neu)

§ 26 Abs. 4 BDSG (neu)

„Die Verarbeitung personenbezogener Daten, **einschließlich besonderer Kategorien personenbezogener Daten** von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten."

Abs. 5: Der Arbeitgeber muss durch **geeignete Maßnahmen** sicherstellen, dass die allgemeinen **datenschutzrechtlichen Grundsätze** des Art. 5 DS-GVO eingehalten werden