HOECK SCHLÜTER VAAGT
Rechtsanwälte | Fachanwälte | Notare

Arbeitnehmer-Datenschutz und Compliance

Daten- & Persönlichkeitsschutz im Arbeitsverhältnis

Jan A. Strunk
Rechtsanwalt
Fachanwalt für Arbeitsrecht
Fachanwalt für Informationstechnologierecht

Fachanwaltsfortbildung 2015
Veranstaltung: 11.12.2015 Hannover

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

Who is…

Jan A. Strunk

- Jahrgang 1967
- Rechtsanwalt seit 1999
- Fachanwalt für Arbeitsrecht seit 2008
- Fachanwalt für Informationstechnologierecht (IT-Recht) seit 2009
- Datenschutzauditor (DSA-TÜV zertifiziert)
- Datenschutzbeauftragter (DSB-TÜV zertifiziert)
- Jur. Fachautor, Dozent in der Aus- & Weiterbildung
- Kanzlei: HOECK SCHLÜTER VAAGT Rechtsanwälte Partnerschaft mbB
  Wirtschafts- und Unternehmensrecht, Flensburg
  Speziell: Danish-Desk für deutsch-dänische Rechtsbeziehungen

Blog:

LEGALIT.de
::: IKT | Arbeit | Medien | Recht :::

Beratungs-& Tätigkeits-Schwerpunkte	Informations- und Kommunikationsrecht *(SP: Datenschutz, Internet- & Onlinerecht, Medien- & Social-Media-Recht)*
	Arbeits- und Berufsrecht *(SP: Unternehmen, Kollektivarbeitsrecht)*
	Gewerblicher Rechtsschutz *(SP: Marken-, Urheber- und Wettbewerbsrecht)*
	Corporate Compliance *(rechtlich)*

Zeitplan

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

- 9:30 – 11.00 Uhr
- Pause
- 11:15 – 13:00 Uhr
- Mittagspause
- 14:00 – 15:30
- Pause
- 15:45 – 17:00 Uhr

Arbeitsrecht & Datenschutz

Mittlerweile hohe Praxisrelevanz im betrieblichen Alltag:

= Anwaltlicher Beratungsbedarf!

Betriebsräte zunehmend sensibler
-> Bessere Wahrnehmung der Mitbestimmungsrechte: Verhandlungen bei MBR, aber auch Unterlassungsanträge bei Verstößen des AG gegen DSR

Neuere höchstrichterliche Entscheidungen zum Umgang mit AN-Daten
-> Auch nichtautomatisierter Umgang mit Informationen mittlerweile rechtlich relevant, Klärung des Merkmals *„erforderlich“* im Rahmen des DSR für das Arbeitsverhältnis durch BAG

Arbeitsgerichte verschärfen Rechtsprechungspraxis bei datenschutzrechtlich relevanten Sachverhalten -> Prozessuale Folgen von DSR-Verstößen (Unwirksamkeit von Kündigungen, Beweisverwertungsverbot) *Siehe zuletzt etwa:* ArbG Cottbus, Urt. v. 25.11.2014 - 3 Ca 359/14

Ältere BV u.U. anpassungsbedürftig
-> Unwirksamkeit bei Verstoß gegen vom BAG als Prüfungsmaßstab festgelegten Verhältnismäßigkeitsgrundsatz

Maßnahmen von Datenschutzaufsichtsbehörden
-> Untersagungsverfügungen, Bußgelder, Gewinnabschöpfung

Notwendigkeit praktischer Ausgleich **Compliance-Anforderungen** vs. DSR & PersönlichkeitsR AN

Agenda

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

- VI. Rechtsfolgen bei Verstößen
- V. Informations-/Handlungspflichten des Arbeitgebers
- IV. Betriebsverfassungsrechtliche Rahmenbedingungen der Datenverarbeitung
- III. Datentransfer im Konzern und Zulässigkeit der Weitergabe von AN-Daten an Dritte
- II. Typische Konflikt-/Problemfelder im Unternehmen
- I. Gesetzliche Grundlagen und Systematik des AN-Datenschutzes

Standort

I. **Gesetzliche Grundlagen und Systematik des AN-Datenschutzes**
II. Typische Konfliktfelder im Unternehmen
III. Datentransfer im Konzern und Zulässigkeit der Weitergabe von AN-Daten an Dritte
IV. Betriebsverfassungsrechtliche Rahmenbedingungen der Datenverarbeitung
V. Informations-/Handlungspflichten des Arbeitgebers
VI. Rechtsfolgen bei Verstößen

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

Grundrechtliche Interessenkollisionen im Arbeitsverhältnis (IKT)

Arbeitnehmer

Allgemeines Persönlichkeitsrecht
(informationelle Selbstbestimmung, Schutz des gesprochenen Wortes, Recht auf private Datensphäre / IT-Grundrecht),*
Art. 2 Abs. 1 GG bzw. Art. 1 Abs. 1 GG

Post-/Fernmeldegeheimnis,
Art. 10 Abs. 1 GG

Arbeitgeber

Allgemeines Persönlichkeitsrecht

Eigentum

Recht am eingerichteten und ausgeübten Gewerbebetrieb
Art. 14 GG

Datenschutz schützt Menschen, nicht Daten!

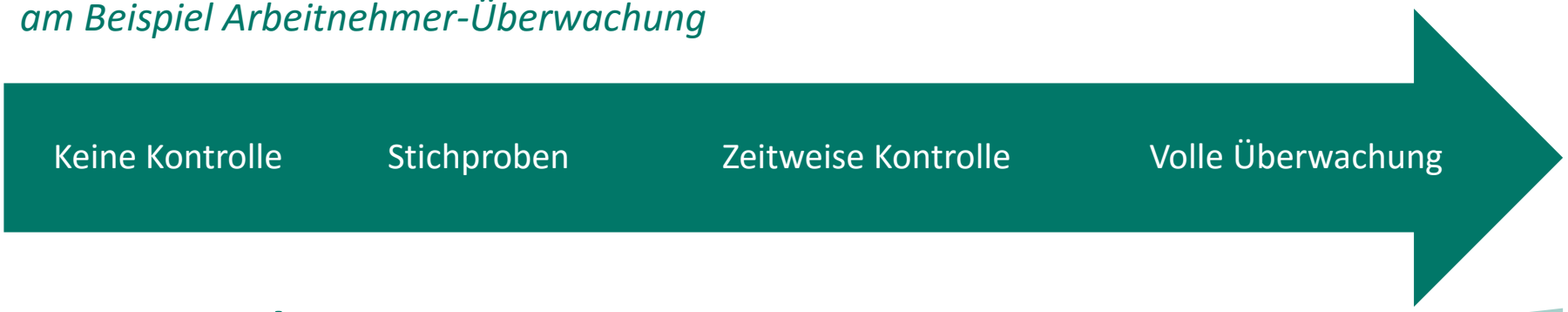
Lösung durch:

- einfachgesetzliche Regelungen
- Einzelfallbezogene Güter- und Interessenabwägung unter Beachtung des Verhältnismäßigkeitsprinzips

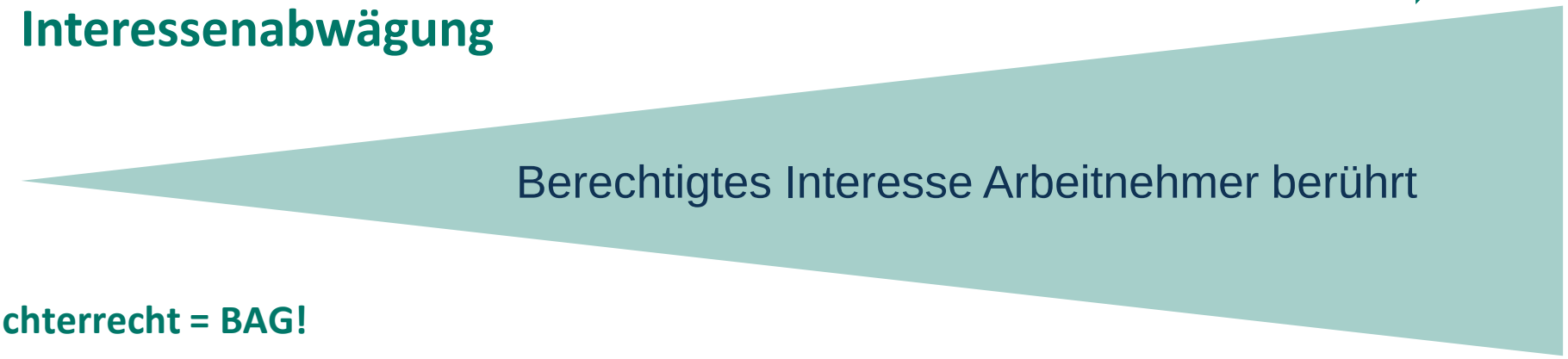
* = Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität" informationstechnischer Systeme“ *(BVerfG, 27.2.2008 - 1 BvR 370/07 + 595/07)*

Basics: Zulässigkeit Grundrechtseingriff

am Beispiel Arbeitnehmer-Überwachung



Interessenabwägung



Richterrecht = BAG!

„Klassische“ Verhältnismäßigkeitsprüfung:

- ✓ **geeignet**, um legitimen Zweck zu verwirklichen?
- ✓ **erforderlich**, da Zweck nicht durch milderen Eingriff in das PersR erreichbar?
- ✓ **angemessen**, da keine überwiegenden schutzwürdigen Belange des Betroffenen?

Arbeitnehmerdatenschutz

„Mit dem Gesetzentwurf soll erstmals seit jahrzehntelanger Diskussion eine umfassende gesetzliche Regelung für den Arbeitnehmerdatenschutz getroffen werden.[…]. Daraus ergibt sich eine hohe Komplexität der Materie und ein erheblicher Beratungsbedarf, der eine Verlängerung der Frist zur Stellungnahme erforderlich macht.„ *[Bundesrat im Oktober 2010]*

Aktueller Stand:

- Auch im Jahr 2015 immer noch kein Gesetz zum Beschäftigten-Datenschutz in Deutschland
- Regelungen zur Zeit nur in vereinzelten Normen verschiedener allgemeiner und bereichsspezifischer Gesetze
- Rechtlicher Rahmen weitgehend nur durch Richterrecht abgesteckt

Arbeitnehmer-Datenschutz = Die unendliche Geschichte – Timeline der letzten sechs Jahre:

- **25. November 2009**: SPD-Fraktion bringt Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG) in den Bundestag ein (BT-Drs. 17/69).
- **31. März 2010**: Bundesinnenministerium legt Eckpunktepapier zum Beschäftigtendatenschutz vor.
- **28. Mai 2010**: Bundesinnenministerium erarbeitet Referentenentwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes.
- **25. August 2010**: Bundeskabinett beschließt Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes (Regierungsentwurf, Bearbeitungsstand: 24.08.2010). => Pressepapier
- **5. November 2010**: Bundesrat nimmt Stellung (BR-Drs. 535/10(B)) zum Gesetzentwurf der Bundesregierung (BR-Drs. 535/10) unter Berücksichtigung der Empfehlungen seiner Ausschüsse (BR-Drs. 535/2/10).
- **25. Februar 2011**: 1. Lesung, Beratung des Regierungsentwurfs zum Gesetz zur Regelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230). Weiterverweisung in die zuständigen Ausschüsse. Ebenfalls erstmalig beraten: Gesetzentwurf von BÜNDNIS 90/DIE GRÜNEN zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen (BT-Drs. 17/4853).
- **18./19. Mai 2011**: Justizministerkonferenz in Halle. Forderung nach Ergänzung des Regierungsentwurfs.
- **23. Mai 2011**: Öffentlichen Sachverständigenanhörung im Innenausschuss des Bundestags. Kontroverse Diskussion des Regierungsentwurfs (BT-Drs. 17/4230). Ebenfalls diskutiert: Gesetzentwürfe der SPD-Fraktion (BT-Drs. 17/69) und der Fraktion BÜNDNIS 90/DIE GRÜNEN (BT-Drs. 17/4853), sowie Anträge der Grünen (BT-Drs. 17/121) und der Fraktion Die Linke (BT-Drs. 17/779).
- **29. September 2011**: Bundestag berät Antrag der SPD-Fraktion zur Regelung des Beschäftigtendatenschutzes in einem eigenen Gesetz (BT-Drs. 17/7176) und überweist ihn in die zuständigen Ausschüsse.
- **9. November 2011:** Die Justizministerinnen und Justizminister der Länder bekräftigen auf ihrer Herbstkonferenz in Berlin am 09.11.2011, dass eine umfassende Regelung des Beschäftigtendatenschutzes dringend erforderlich sei (Beschluss der JuMiKo).
- **26. September 2012:** Die Bundesregierung verteidigt den von ihr vorgelegten Gesetzentwurf. Zu dem Entwurf habe es „zustimmende und ablehnende Stimmen gegeben“, schreibt die Regierung in ihrer Antwort (BT-Drs. 17/10666) auf eine Kleine Anfrage der Fraktion Die Linke (BT-Drs. 17/10540). Sie nehme jede Kritik ernst, halte ihren Gesetzentwurf in der vorgelegten Fassung aber „weiterhin für ausgewogen und in der Sache richtig“.
- **29. Januar 2013:** Die Regierungskoalition nimmt die für den 01.02.2013 geplante Abstimmung des Bundestages über den Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes von der Tagesordnung und kündigt weitere Gespräche mit allen Beteiligten an.
- **26. Februar 2013:** Die Bundesregierung stoppt das Gesetzesvorhaben vorläufig (dpa-Meldung).
- **5. Juli 2013:** Der Bundesrat beschließt auf Antrag des Landes Baden-Württemberg eine Entschließung (BR-Drs. 552/13). Darin wird die Bundesregierung aufgefordert, in dem Verfahren auf Erlass einer Datenschutz-Grundverordnung der EU auf die Grundlagen für einen effektiven Beschäftigtendatenschutz durch den nationalen Gesetzgeber hinzuwirken. Seitdem: Still ruht der See…
- **01.04.2015**: Empfehlungen des Europarates zur besseren Absicherung der informationellen Selbstbestimmung am Arbeitsplatz. Bloße Handlungsempfehlungen = Soft law

Basics: Technische Überwachung

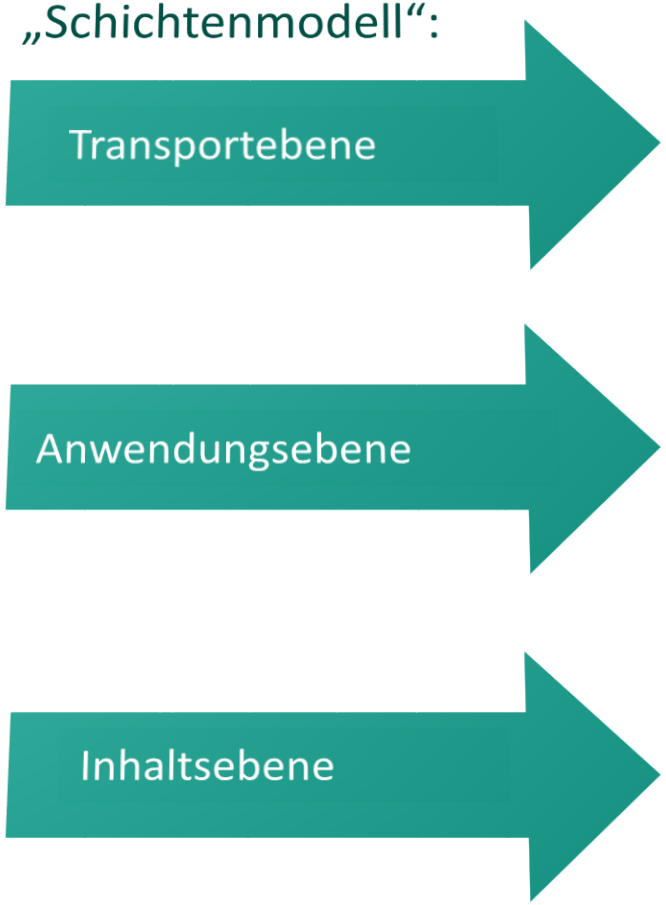
Drei Phasen der Personaldaten-verarbeitung:

- **Sammeln**
  „Ermittlungsphase“
- **Sichten & Ordnen**
  „Verarbeitungsphase“
- **Beurteilen & Bewerten**
  „Analysephase“

Arbeitsrechtliche Reaktion auf Feststellungen ist nicht mehr Teil des Überwachungsvorgangs

Basics: Herkömmliche Funktionelle Einteilung von Datenschutznormen (DS-Behörden)

„Schichtenmodell“:



Technik der Informationsübermittlung

- Bereitstellung von Leitungen und Netzknoten
- e-Mail, Internetzugang
- Voice over IP

= Telekommunikationsgesetz TKG

Telemediendienste

- Anbieten elektronischer Informations- und Kommunikationsdienstleistungen (soweit nicht ausschließlich dem TKG zuzuordnen)

= Telemediengesetz TMG,

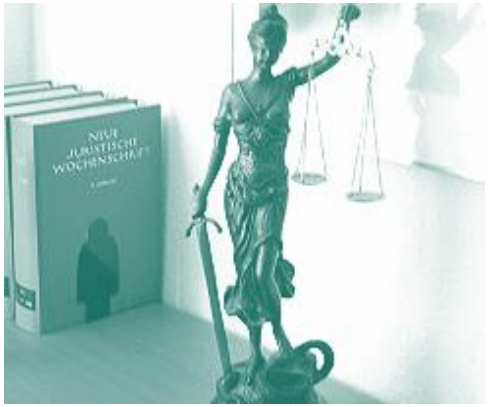
ggf. Rundfunkstaatsvertrag RStV (für redaktionell bearbeitete Inhalte sowie Rundfunk/Fernsehen)

Übertragene Informationen

- Nachrichten, Gesprächsinhalte
- Inhalte von aufgerufenen Seiten
- Voice over IP

= Datenschutzgesetze, insbes. BDSG

Datenschutzrechtlich relevante Normen bei der IKT-Nutzung in Unternehmen



[Landes-datenschutzgesetze]

Allgemeines Gleichbehandlungs-gesetz

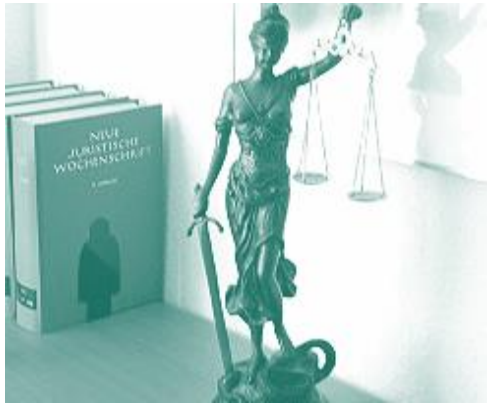
Bundes-datenschutzgesetz

Rundfunk-staatsvertrag

Tele-kommunikations-gesetz

Telemediengesetz

TKG



[P] Ausdrückliche Gestattung oder stillschweigende Duldung der **Privatnutzung**:

Arbeitgeber ist nach wohl **noch** überwiegender Ansicht TK-Dienstanbieter, der dem Fernmeldegeheimnis unterliegt!

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

§ 3 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

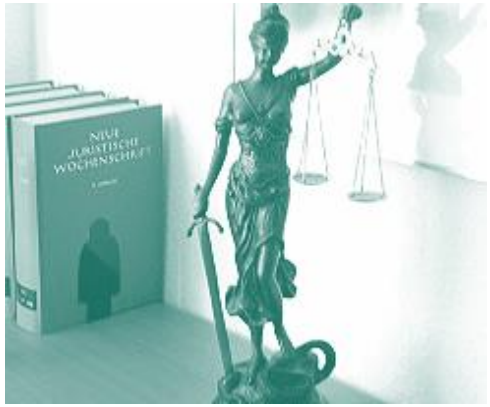
6. "Diensteanbieter" jeder, der **ganz oder teilweise geschäftsmäßig**
a) Telekommunikationsdienste erbringt oder
b) an der Erbringung solcher Dienste mitwirkt;

10. "geschäftsmäßiges Erbringen von Telekommunikationsdiensten" das nachhaltige Angebot von Telekommunikation **für Dritte** mit oder ohne Gewinnerzielungsabsicht;

22. "Telekommunikation" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen;

a.A. Rechtsprechung: LAG Berlin-Brandenburg, 16.02.2011 (4 Sa 2132/10), LAG Niedersachsen, 31.05.2010 (12 Sa 875/09), VG Karlsruhe, 27.05.2013 – 2 K 3249/12 „Mappus“.

Datenschutzrechtliche Regelungen des TMG



Normen: §§ 11-15

Aber:

Bei gestatteter Privatnutzung liegt Nutzungszweck außerhalb des Arbeitsverhältnisses vor

–> Damit **Anwendbarkeit des TMG**!

- Relevant i.d.R. nur bei Mediendiensten im „Außenverhältnis“, z.B. Firmenwebsite

  Dann bedeutsam: Pflichtangaben, Haftung für Inhalte (auch: RStV)

- Datenschutzrechtliche Bestimmungen des TMG im Arbeitsverhältnis grds. nicht anwendbar:

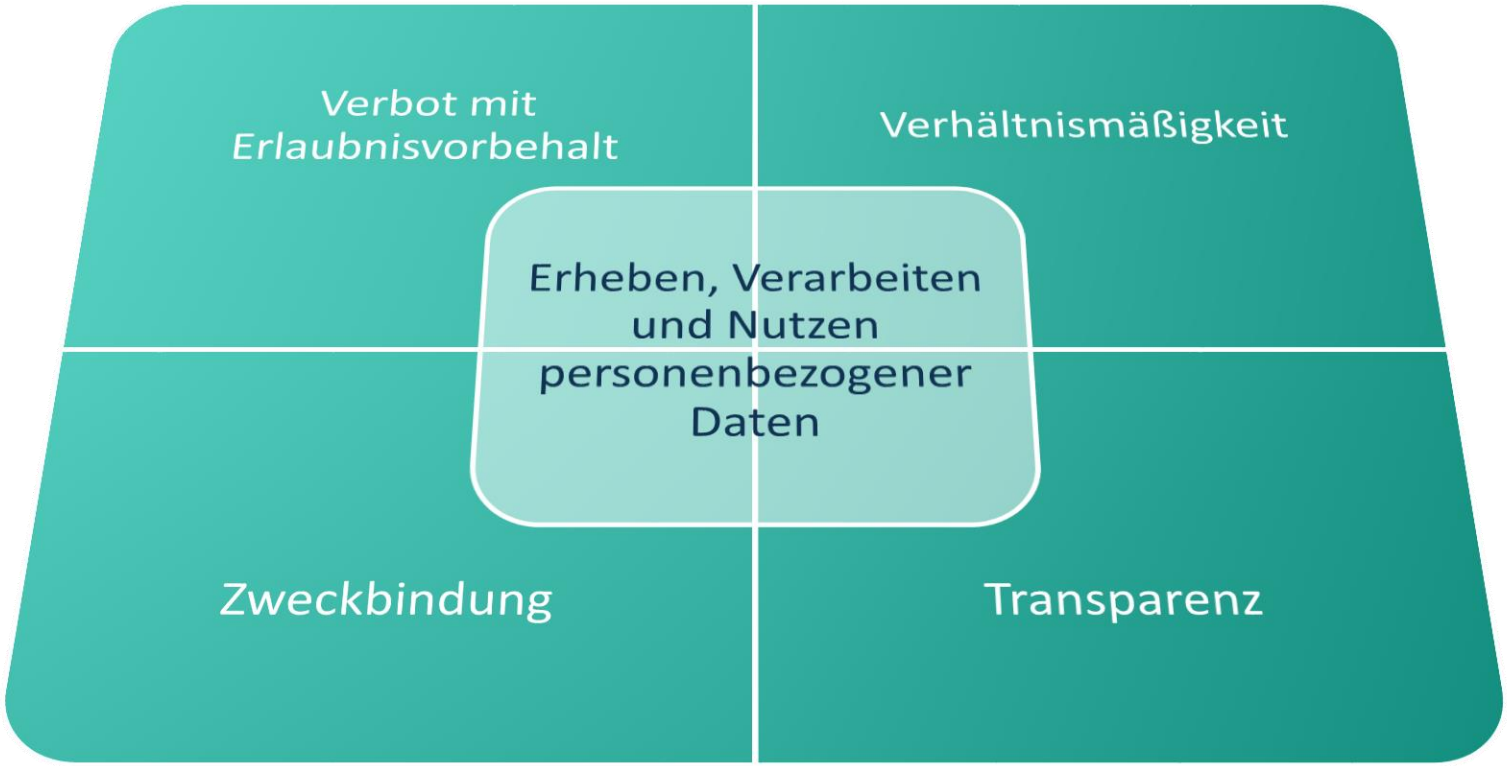
§ 11 TMG Anbieter-Nutzer-Verhältnis

(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

Basics: Das BDSG im Überflug…



Zweckbindung: Kein Anspruch auf Auskunft über Privatadresse eines angestellten Arztes

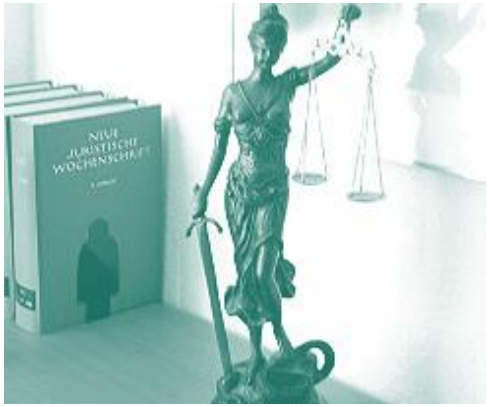
-> BGH, Urteil v. 20.01.2015 - VI ZR 137/14

Arbeitgeber müssen & dürfen die Daten ihrer Arbeitnehmer nicht zur Vorbereitung eines Gerichtsverfahrens an Dritte herausgeben

Wesentlicher Sachverhalt:
In dem Verfahren ging es ursprünglich um die Zustellung einer Klage in einem Arzthaftungsprozess. Der Kläger wollte hierfür von der beklagten Klinik die Privatanschrift seines behandelnden Arztes erfahren. Diese weigerte sich jedoch und der geschädigte Patient klagte auf Auskunftserteilung.
Das Amtsgericht hatte die Klage abgewiesen, das Landgericht dagegen die Beklagte zur Auskunft verurteilt, weil sich Anonymität nicht mit dem Wesen des Arzt-Patienten-Verhältnis vertrage.

Aus der Entscheidung:
Zwar hat der Patient gegenüber Arzt und Krankenhaus grundsätzlich auch außerhalb eines Rechtsstreits Anspruch auf Einsicht in die ihn betreffenden Krankenunterlagen, soweit sie Aufzeichnungen über objektive physische Befunde und Berichte über Behandlungsmaßnahmen (Medikation, Operation etc.) betreffen. Der Klinikträger ist deshalb grundsätzlich gehalten, dem Patienten den Namen des ihn behandelnden Arztes mitzuteilen. […]. Die darüber hinaus verlangte Mitteilung der Privatadresse des Arztes ist für den Kläger zur Verfolgung seiner Ansprüche nicht erforderlich. […]. Zur Führung des bereits rechtshängigen Prozesses bedarf der Kläger der Privatanschrift nicht.
Der Auskunftserteilung steht ferner die datenschutzrechtliche Vorschrift des § 32 Abs. 1 Satz 1 BDSG der Auskunftserteilung entgegen. Die Regelung gestattet dem Arbeitgeber die Erhebung, Verarbeitung und Nutzung von Daten für Zwecke des Beschäftigungsverhältnisses. Der Arbeitgeber ist aber grundsätzlich nicht berechtigt, personenbezogene Daten, die für Zwecke des Beschäftigungsverhältnisses erhoben worden sind, an Dritte weiterzuleiten.
Da die Daten für die Zwecke des Beschäftigungsverhältnisses erhoben worden sind, ist die Übermittlung an Dritte nach dem für den Datenschutz geltenden Zweckbindungsgebot grundsätzlich als zweckfremde Verwendung ausgeschlossen.

BDSG- Basics:



Grundsatz der Datensparsamkeit:

„So wenig Daten wie möglich, nur so viele, wie erforderlich!“

- Rein technischer Ansatz
- **[P]: Zeitgemäß?**

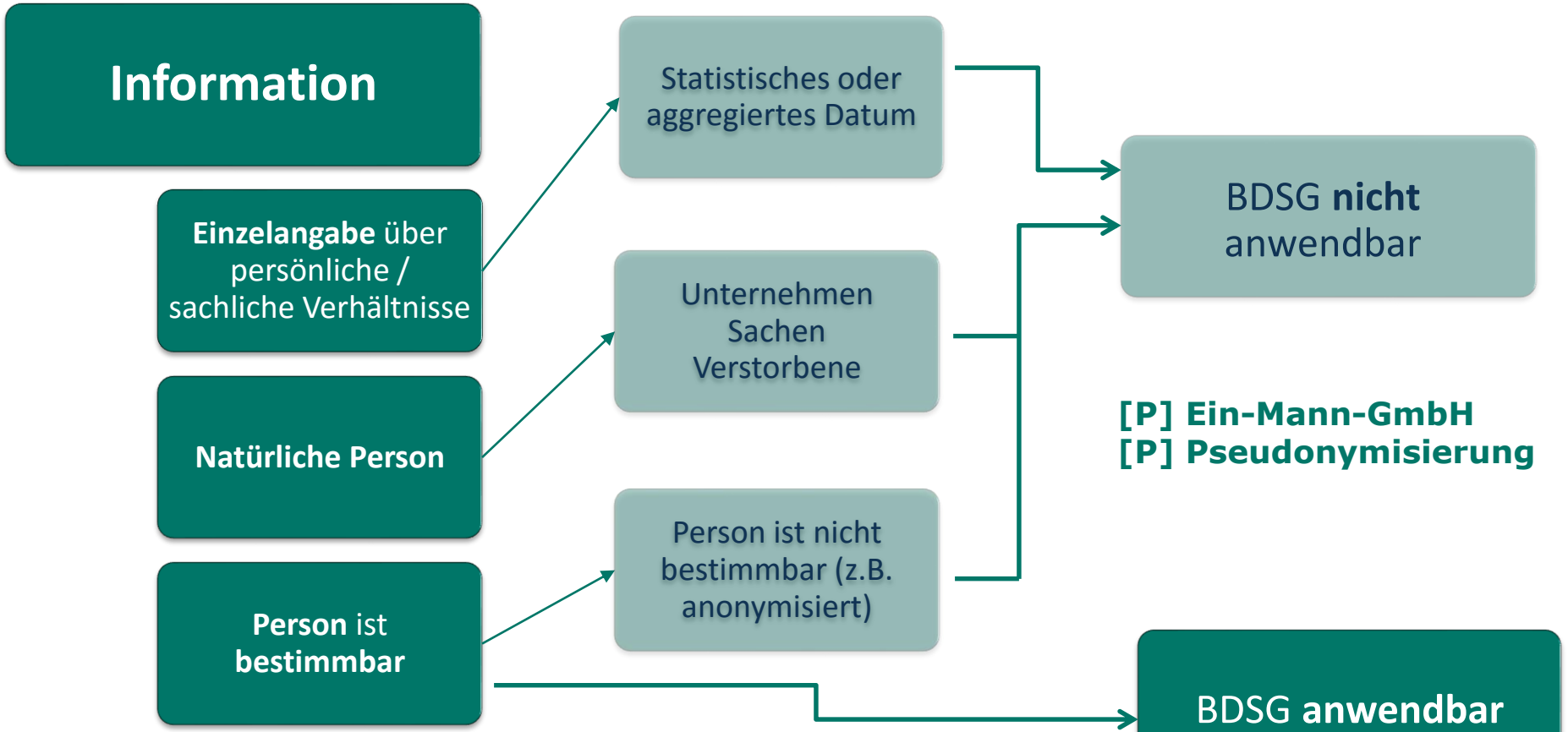
§ 3a Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Ansatz: **„Datenschutz durch Technik“**
- Praktisch unverbindliche Zielvorgabe
- Verstoß als solcher sanktionslos

Personenbezogene Daten, § 3 Abs. 1 BDSG



§ 3 Abs. 9 BDSG: „sensible Daten"=> Besonderer Schutz (auch mittelbare Daten, z.B. Fehltage-Liste)

Basics: § 3 BDSG

§ 3 Weitere Begriffsbestimmungen

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

(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.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. […].

(11) Beschäftigte sind:

1.Arbeitnehmerinnen und Arbeitnehmer,

2.zu ihrer Berufsbildung Beschäftigte, […],

8. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, […].

Personen:

- **Betroffener** (Abs.1)
- **Verantwortliche Stelle** (Abs. 7)
- **Empfänger** (Abs. 8)
- **Dritter** (Abs. 8)
- **Beschäftigte** (Abs. 11)

Arten personenbezogener Daten

• **Bestandsdaten** = Daten, die in einem Kommunikationsdienst oder –netz dauerhaft gespeichert sind, z.B. e-Mail-Adresse, Benutzerkennung, Paßwort oder (statische) IP-Adresse

• **Verbindungsdaten / „Verkehrsdaten“** (§ 3 Nr. 30 TKG) = Angaben über die Kommunikationspartner des jeweiligen Dienstes, z.B. Telefonnummern, e-Mail-Adressen sowohl des Anrufers / Angerufenen als auch des Absenders / Empfängers. Angaben über Zeitpunkt und Dauer einer Verbindung, in Anspruch genommene Systemleitungen, benutzte Anschlüsse etc.

• **Entgelt-/Abrechungsdaten** = Daten, die (nur) zu Abrechnungszwecken verarbeitet werden

• **Inhaltsdaten** = übertragene Informationen und Nachrichten (z.B. per e-Mail oder Telefon), die einem bestimmten Empfänger oder Absender zugeordnet werden können. Auch: Inhalte aufgerufener Webseiten.

• **Besondere Arten personenbezogener Daten** (§ 3 Abs. 9 BDSG)
= Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

§ 3 BDSG – Überblick:

Umgang mit personenbezogenen Daten

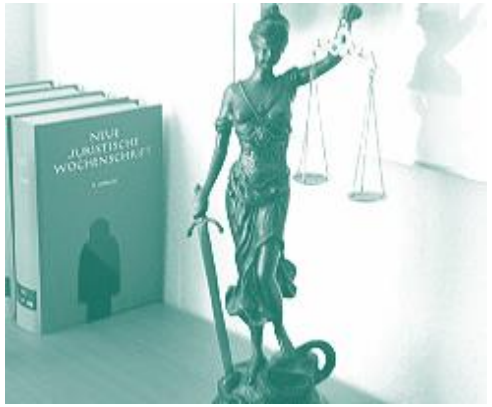
Erheben	Verarbeiten					Nutzen
= Beschaffen von Daten § 3 Abs. 3	**Speichern** § 3 Abs. 4 Satz 2 Nr. 1	**Verändern** § 3 Abs. 4 Satz 2 Nr. 2	**Übermitteln** § 3 Abs. 4 Satz 2 Nr. 3	**Sperren** § 3 Abs. 4 Satz 2 Nr. 4	**Löschen** § 3 Abs. 4 Satz 2 Nr. 5	Auffang-Tatbestand § 3 Abs. 5

Verarbeiten: 5 Fallgruppen:

Anonymisieren §3 Abs. 6

Pseudonymisieren §3 Abs. 6a

Basics: § 4 BDSG



Verbot mit „Erlaubnisvorbehalt“:

Für Datenverarbeitung daher stets erforderlich:

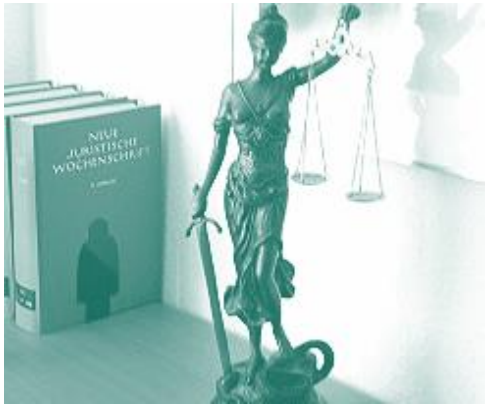
Gesetzliche Erlaubnis oder Einwilligung

§ 4 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.

Basics: § 4a BDSG



Arbeitnehmer muß

- durch AG über die Tragweite seiner Einwilligung **hinreichend** informiert worden sein

und

- die **tatsächliche** Möglichkeit haben, sie ohne Angst vor Sanktionen abzulehnen oder später zu widerrufen

Grundsatz der „informierten Einwilligung“:

§ 4a Einwilligung

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

Einwilligung sollte arbeitgeberseitig nur dann eingeholt werden, wenn die beabsichtigte Verarbeitung personenbezogener Daten nicht durch Gesetz (oder TV bzw. BV!) bereits erlaubt ist.

Freiwilligkeit der Einwilligung im Arbeitsverhältnis

Aktuelle Grundsatz-entscheidung

BAG, Urteil vom 11.12.2014, 8 AZR 1010/13:

„**Auch im Rahmen eines Arbeitsverhältnisses können Arbeitnehmer sich grundsätzlich „frei entscheiden", wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben wollen**. Dem steht weder die grundlegende Tatsache, dass Arbeitnehmer abhängig Beschäftigte sind noch das Weisungsrecht des Arbeitgebers, § 106 GewO, entgegen. Mit der Eingehung eines Arbeitsverhältnisses und der Eingliederung in einen Betrieb begeben sich die Arbeitnehmer nicht ihrer Grund- und Persönlichkeitsrechte. Die zu § 4a BDSG formulierte Gegenauffassung *(Simitis in Simitis BDSG 8. Aufl. § 4a Rn. 62)* verkennt, dass schon nach § 32 BDSG Datenverarbeitung im Arbeitsverhältnis möglich ist, unter den Voraussetzungen des § 32 BDSG sogar einwilligungsfrei. Löste die Verweigerung einer außerhalb von § 32 BDSG erforderlichen schriftlichen Einwilligung Benachteiligungen aus, so stellte dies einen groben Verstoß gegen die arbeitgeberseitigen Pflichten aus § 241 Abs. 2 und § 612a BGB dar, der zum Schadensersatz nach §§ 282, 280 Abs. 1 BGB verpflichtete."

„Wegen der Bedeutung des Rechts der Arbeitnehmer, auch im Arbeitsverhältnis ihr Grundrecht auf informationelle Selbstbestimmung ausüben zu dürfen, führt eine solche Abwägung im Ergebnis dazu, dass **auch und gerade im Arbeitsverhältnis die Einwilligung der Arbeitnehmer der Schriftform bedarf**. Nur dadurch kann verdeutlicht werden, dass die Einwilligung der Arbeitnehmer zur Veröffentlichung ihrer Bildnisse unabhängig von den jeweiligen Verpflichtungen aus dem eingegangenen Arbeitsverhältnis erfolgt und dass die Erteilung oder Verweigerung der Einwilligung für das Arbeitsverhältnis keine Folgen haben dürfen."

„Allerdings deutet ein Umkehrschluss aus § 28 Abs. 3a Satz 1 aE BDSG darauf hin, dass **eine einmal erteilte Einwilligung nicht generell „jederzeit mit Wirkung für die Zukunft widerrufen werden kann".** […]. Es ist wiederum im Rahmen der gegenseitigen Rücksichtnahme auf die Interessen der anderen Seite, § 241 Abs. 2 BGB, eine Abwägung im Einzelfall vorzunehmen. […]. Im Ergebnis der in solchen Fällen vorzunehmenden Gesamtabwägung ist vielmehr zu verlangen, dass der widerrufende Arbeitnehmer einen Grund im Sinne einer Erklärung angibt, warum er nunmehr[…] sein Recht auf informationelle Selbstbestimmung gegenläufig ausüben will."

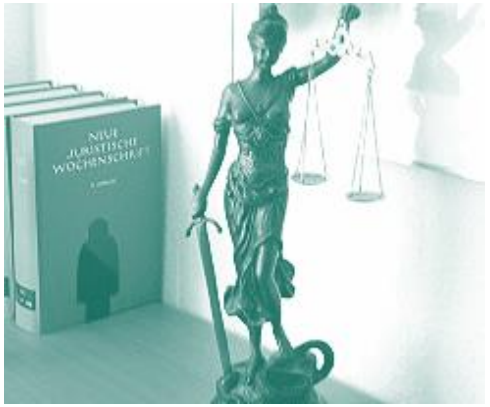
Überblick:
Spezifische Erlaubnistatbestände des BDSG für das Arbeitsverhältnis

Umgang mit Beschäftigtendaten

- Zwecke des Beschäftigungsverhältnisses — § 32 Abs. 1 Satz 1
- Aufdeckung von Straftaten — § 32 Abs. 1 Satz 2
- Wahrung berechtigter Interessen — § 28 Abs. 1 Satz 1 Nr. 2

Basics: § 28 BDSG

Befugnis zum Erheben, Speichern und Nutzen von Daten



Im Rahmen der Zweckbestimmung dürfen personenbezogene Daten ohne Einwilligung des Betroffenen erhoben verarbeitet und genutzt werden!

§ 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

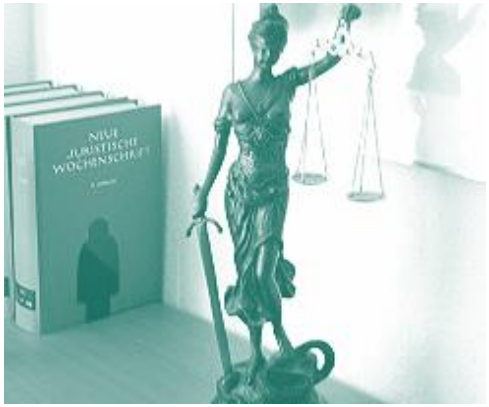
(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel **für die Erfüllung eigener Geschäftszwecke** ist zulässig
1. **wenn** es der **Zweckbestimmung** eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
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.

Weitere spezifische Befugnisse ergeben sich bei erlaubter Privatnutzung nach bislang h.M. insbesondere aus § 95 Abs. 1 TKG, § 96 Abs. 1 TKG sowie § 100 Abs. 3 TKG

Basics: § 32 BDSG

Befugnis zum Erheben, Speichern und Nutzen von Daten im Arbeitsverhältnis



"Lex Lidl": Legislative Reaktion auf Datenschutz-Skandale -> Erst mit der Entwurfsfassung vom 01.07.2009 noch kurzfristig in die BDSG-Novelle II eingefügt…

§ 32 BDSG: **Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses**

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Basics: § 32 BDSG

[P] Durchführung rein präventiver Kontrollen

ArbG Cottbus, Urt. v. 25.11.2014 - 3 Ca 359/14: Beweisverwertungsverbot bei ohne konkreten Verdacht erhobenen Daten

Befugnis zum Erheben, Speichern und Nutzen von Daten im Arbeitsverhältnis gem. § 32 Abs. 1 BDSG:

Zwecke	• Begründung, Durchführung, Beendigung des ArbV (Satz 1) • Aufdeckung einer Straftat (Satz 2)
Art des Umgangs mit personenbezogenen Daten	• Jede Form der Datenerhebung, auch analog, § 32 Abs. 2 BDSG
betroffener Personenkreis	• Alle abhängig Beschäftigten i.S.d. § 3 Abs. 11 BDSG
Rechtmäßigkeitsvoraussetzungen	• Erforderlichkeit (Satz 1) • Konkreter Tatverdacht, Erforderlichkeit, Verhältnismässigkeit (Satz 2)

„Spindkontrolle“ – BAG, 20.06.2013 (2 AZR 546/12 „Höschen-Urteil“)

Klarstellung, die außer auf i.S.d. § 32 Abs 1 S. 2 BDSG auch auf andere Normen des BDSG übertragen werden kann:

Erforderlich kann eine **Datenverarbeitung nur** sein, **wenn** sie gemäß den Grundsätzen des öffentlichen Rechts **verhältnismäßig** ist, was sich nach den klassischen Kriterien

legitimer Zweck,

Geeignetheit,

Erforderlichkeit und

Angemessenheit beurteilt.

Das allgemeine Interesse an einer funktionstüchtigen Rechtspflege und das Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, reichen für sich betrachtet nicht aus, dem Verwertungsinteresse im Rahmen der Angemessenheitsprüfung vorzunehmenden Abwägung den Vorzug zu geben.

Explizit angesprochen:

§ 32 Abs. 2 BDSG hebt grundsätzliche Beschränkung der Anwendung des BDSG auf dateigebundene bzw. automatisierte Verarbeitungen auf und erfasst auch die Datenerhebung durch rein tatsächliche Handlungen:

Öffnen eines dem AN persönlich zugeordneten Schranks ohne Einwilligung zwecks Durchsuchung ist regelmäßig ein schwerwiegender Eingriff in die Privatsphäre, der nur bei Vorliegen zwingender Gründe gerechtfertigt ist.

Unbeantwortet:

Spindöffnung = Datenerhebung und -verarbeitung im Sinne des § 32 Abs. 1 BDSG?

Wenn (+), Voraussetzungen des § 32 Abs. 1 S. 2 BDSG zu beachten:

„ Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind“

„Spindkontrolle“ = Grundsatzurteil zu Beweisverwertungsverbot

-> BAG, Urteil v. 20.06.2013 - 2 AZR 546/12 („Höschen-Urteil“)

Praktische Bedeutung: „fruit of the poisonous tree“ im Arbeitsrecht...

Leitsätze

Der prozessualen Verwertung von Beweismitteln, die der Arbeitgeber aus einer in Abwesenheit und ohne Einwilligung des Arbeitnehmers durchgeführten Kontrolle von dessen Schrank erlangt hat, kann schon die Heimlichkeit der Durchsuchung entgegenstehen.

Hat der Arbeitgeber dem Betriebsrat bestimmte Kündigungsgründe nicht mitgeteilt, ist sein entsprechender Sachvortrag im Kündigungsschutzprozess gleichwohl verwertbar, wenn der Arbeitnehmer die ordnungsgemäße Anhörung des Betriebsrats erklärtermaßen nicht rügt.

Grundsätzliche Aussagen:

(1) Die Zivilprozessordnung kennt für rechtswidrig erlangte Informationen oder Beweismittel kein - ausdrückliches - prozessuales Verwendungs- bzw. Verwertungsverbot. Aus § 286 ZPO i.V.m. Art. 103 Abs 1 GG folgt im Gegenteil die grundsätzliche Verpflichtung der Gerichte, den von den Parteien vorgetragenen Sachverhalt und die von ihnen angebotenen Beweise zu berücksichtigen. Dementsprechend bedarf es für die Annahme eines Beweisverwertungsverbots, das zugleich die Erhebung der angebotenen Beweise hindern soll, einer besonderen Legitimation in Gestalt einer gesetzlichen Grundlage.

(2) Der persönliche Schrank eines Arbeitnehmers und dessen Inhalt sind Teil der Privatsphäre. Sie sind gleichwohl nicht unter allen Umständen einer Kontrolle durch den Arbeitgeber entzogen. Betroffen ist nicht der absolut geschützte Kernbereich privater Lebensgestaltung, sondern der nur relativ geschützte Bereich des allgemeinen Persönlichkeitsrechts. Stellt der Arbeitgeber dem Arbeitnehmer einen abschließbaren Schrank zur Verfügung, berührt diese Überlassung auch seine eigenen Belange.

(3) Arbeitnehmer müssen darauf vertrauen können, dass ihnen zugeordnete Schränke nicht ohne ihre Einwilligung geöffnet, dort eingebrachte persönliche Sachen nicht ohne ihr Einverständnis durchsucht werden. Geschieht dies dennoch, liegt regelmäßig ein schwerwiegender Eingriff in ihre Privatsphäre vor. Er kann nur bei Vorliegen zwingender Gründe gerechtfertigt sein. Bestehen konkrete Anhaltspunkte für eine Straftat und zählt der Arbeitnehmer zu dem anhand objektiver Kriterien eingegrenzten Kreis der Verdächtigen, kann sich zwar aus dem Arbeitsvertrag i.V.m. § 242 BGB eine Verpflichtung ergeben, Aufklärungsmaßnahmen zu dulden. Erforderlich i.S.d. § 32 Abs 1 S 2 BDSG bzw. verhältnismäßig im Sinne einer Beschränkung des allgemeinen Persönlichkeitsrechts kann eine Schrankkontrolle aber nur sein, wenn sie geeignet, erforderlich und angemessen ist.

(4) Sowohl die Gerichte für Arbeitssachen als auch die ordentlichen Gerichte sind befugt, Erkenntnisse zu verwerten, die sich eine Prozesspartei durch Eingriffe in das allgemeine Persönlichkeitsrecht verschafft hat, wenn eine Abwägung der beteiligten Belange ergibt, dass das Interesse an einer Verwertung der Beweise trotz der damit einhergehenden Rechtsverletzung das Interesse am Schutz der Daten überwiegt. Das allgemeine Interesse an einer funktionstüchtigen Rechtspflege und das Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, reichen dabei für sich betrachtet nicht aus, dem Verwertungsinteresse den Vorzug zu geben.

Standort

I. Gesetzliche Grundlagen und Systematik des AN-Datenschutzes

II. Typische Konfliktfelder im Unternehmen

III. Datentransfer im Konzern und Zulässigkeit der Weitergabe von AN-Daten an Dritte

IV. Betriebsverfassungsrechtliche Rahmenbedingungen der Datenverarbeitung

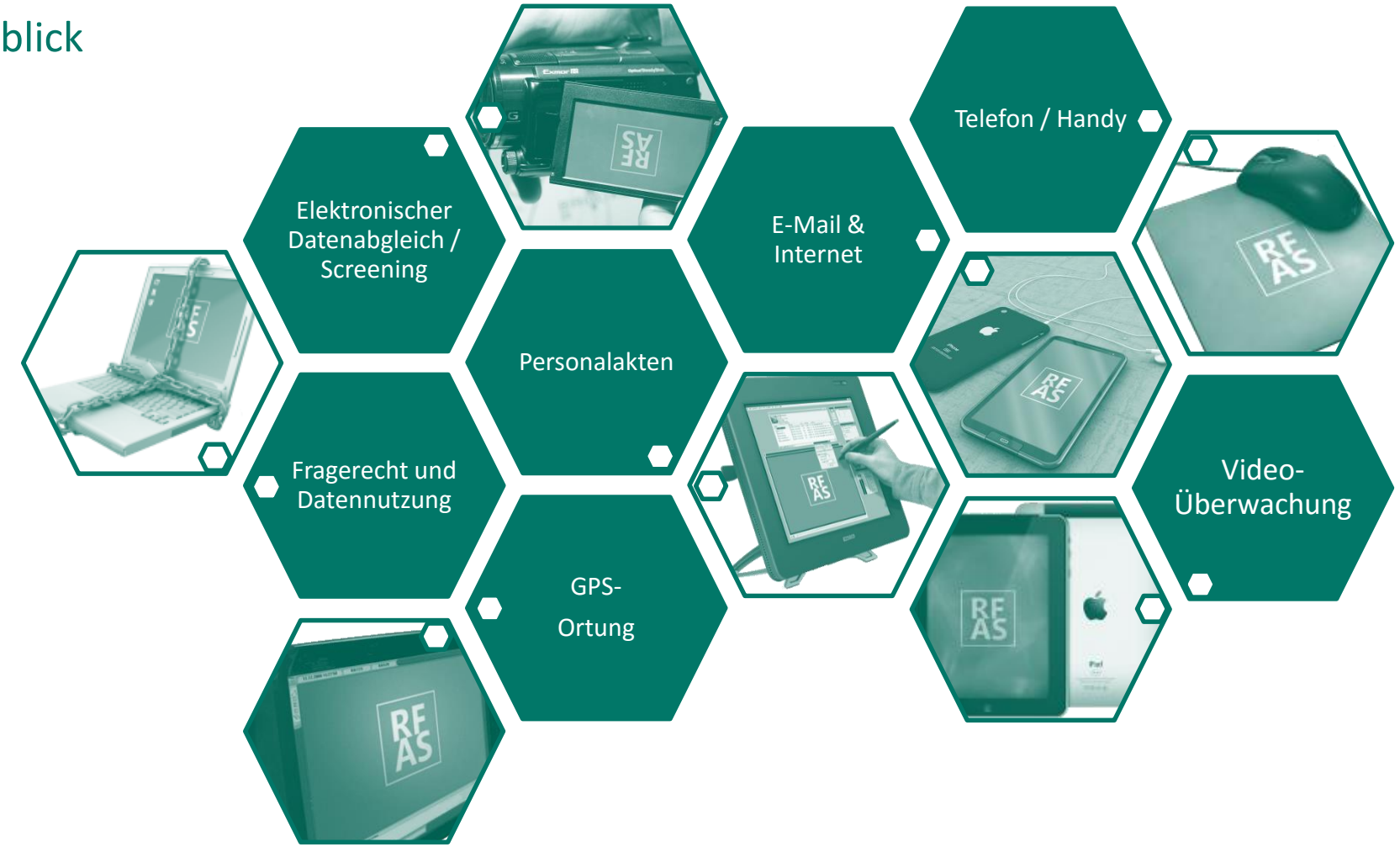
V. Informations-/Handlungspflichten des Arbeitgebers

VI. Rechtsfolgen bei Verstößen

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

Typische Konfliktfelder im Unternehmen

Überblick



Stichwort: „Compliance“ (rechtlich)

Wer, wie, was? - Wieso, weshalb, warum?

Begriff: „Gesetzestreue“, „Einhaltung“, „Befolgung“ des zu beachtenden Rechts

= Sicherstellung rechtskonformen Handelns eines Unternehmens durch sein Management

In den USA umfangreiche interne Ermittlungen, bei international tätigen Unternehmen auch grenzüberschreitende Durchführung -> Strafzahlungen

Verstöße auch auf nationaler Ebene sogar strafrechtlich relevant:
BGH, Urteil v. 17.07.09 – 5 StR 394/08 (Garantenpflicht eines Leiters der Innenrevision)

Seit 2002 Deutscher Government Kodex:
Umsetzung & Einhaltung „Best Practice“
ist Vorstandspflicht
www.corporate-governance-code.de

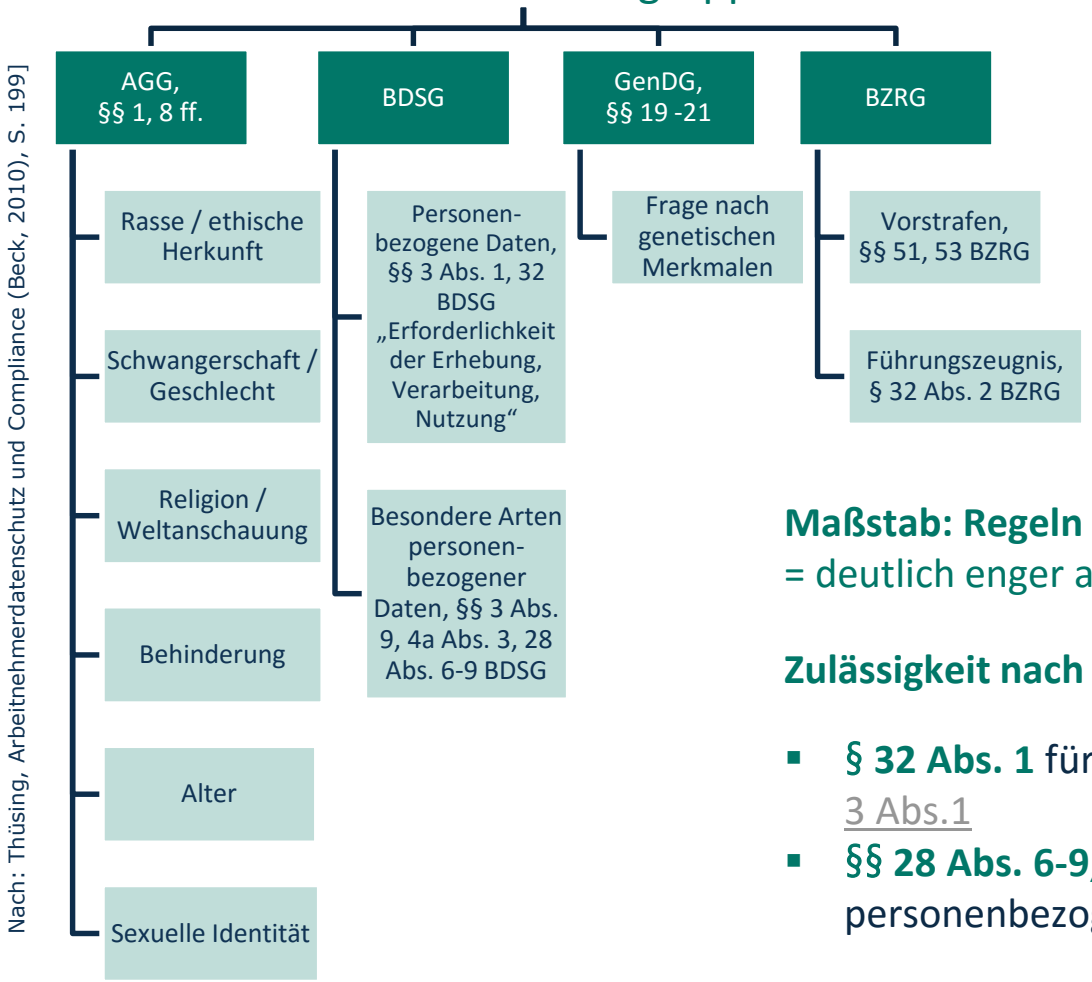
Compliance Regelungen erfüllen Verpflichtungen & haben Schutzfunktion für Unternehmen und seine Verantwortungsträger: **Risikominimierung, Information, Kontrolle**

Compliance-Themen im Arbeitsrecht:	**Persönlichkeitsrechtsschutz**: AGG, [P] Ethikrichtlinien, [P] „Whistleblowing“, AN-Überwachung (Video, E-Mail, Telefon, Datenabgleich / „Screening“),
	Datenschutz (insbes. auch Compliance-Überwachung selbst!)
	Arbeitssicherheit / Arbeitsschutz
	Kollektives Arbeitsrecht: BetrVG, TVG

Compliance-Management-System (CMS) ist auch **Bewertungsfaktor:** Banken, Versicherungen, Investoren

1. Fragerecht und Datennutzung

Schutzebenen & Fallgruppen



Maßstab: Regeln des Anti-Diskriminierungsrechts
= deutlich enger als APR!

Zulässigkeit nach BDSG:

- **§ 32 Abs. 1** für personenbezogene Daten gem. § 3 Abs.1
- **§§ 28 Abs. 6-9**, 4a Abs. 3 für besondere Arten personenbezogener Daten gem. §3 Abs. 9

1. Fragerecht und Datennutzung – Exkurs: Gesundheitsdaten

Erhebung von Gesundheitsdaten im Bewerbungsverfahren

Arbeitsunfähigkeitsbescheinigung

Krankenrückkehrgespräche

Betrieblicher Gesundheitsschutz

Datenschutz

Gesundheitsdaten = besonders sensible Daten i.S.v. § 3 Abs. 9 BDSG

- Wirksame Einwilligung des AN erfordert, dass sich die schriftliche Einwilligungserklärung ausdrücklich auf diese Daten bezieht
- Löschungspflicht für Arbeitgeber gem. § 35 Abs. 2 S. 1 BDSG, wenn er Richtigkeit von Gesundheitsdaten nicht beweisen kann
  => Ausreichend, dass AN Richtigkeit bestreitet, da AG andernfalls durch bewusste Speicherung falscher Daten die Offenbarung der richtigen Daten durch den AN erreichen könnte

1. Fragerecht und Datennutzung: Fragerecht

(Un)Zulässigkeit von Fragen gemessen am Employment Discrimination Law der USA

Gegenstand	Zulässige Frage vor Einstellung	Regelmäßig unzulässige Frage vor Einstellung
Name	Was ist ihr vollständiger Name? Haben Sie je unter diesem oder einem anderen Namen für die Firma gearbeitet?	Was ist ihr Geburtsname? – kann auf Diskriminierung wegen Familienstand oder sexueller Orientierung hindeuten (fehlende Heirat/Geschlechtsumwandlung)
Geburtsort		Eigener Geburtsort oder der von Verwandten: Mögliche Rassendiskriminierung.
Alter	Sind Sie über 18 Jahre alt? – zulässig, wenn Volljährigkeit erforderlich ist für die zu besetzende Position	Wie alt sind Sie?
Glaube oder Religion		Frage nach Religion gänzlich verboten. Frage nach religiösen Praktiken ebenfalls. Möglicher Konflikt auch bei Fragen nach der Verfügbarkeit am Samstag/Sonntag – Rechtfertigung erforderlich
Rasse oder Hautfarbe		Hinweis auf direkte Diskriminierung wegen der ethnischen Zugehörigkeit; ebenso: Frage nach der Hautfarbe des Ehepartners
Fotographie		In den USA stets unzulässig – zuweilen mit Ausnahme: Modell oder Filmindustrie. Ansonsten Hinweis auf mögliche Rassendiskriminierung und Altersdiskriminierung
Größe		Kann auf eine mittelbare Alters-, Behinderten-, Rassen- und Geschlechtsdiskriminierung hindeuten.
Gewicht		Kann auf eine mittelbare Alters-, Behinderten- und Geschlechtsdiskriminierung hindeuten.
Familienstand	Ist Ihr Ehepartner bei uns beschäftigt?	Sind Sie verheiratet? – kann auf eine Diskriminierung wegen sexueller Orientierung hindeuten. Wie heißt ihr Ehepartner? – kann auf eine Rassendiskriminierung hindeuten

Gegenstand	Zulässige Frage vor Einstellung	Regelmäßig unzulässige Frage vor Einstellung
Behinderung		Jede Frage hinsichtlich des aktuellen oder ehemaligen Gesundheitszustands, die nicht direkt berufsbezogen sind und die nicht auf einer gerechtfertigten Unterscheidung beruhen. Jeder Gesundheitstest vor Einstellung kann auf Diskriminierung wegen Behinderung hindeuten.
Nationalität	Können Sie die Tätigkeit legal am gewünschten Arbeitsort verrichten?	Sind sie Deutscher oder Bürger eines anderen EU-Landes? – kann auf Diskriminierung wegen ethnischer Zugehörigkeit hindeuten
Sprachkenntnisse	Sprechen Sie fließend Englisch? Sprechen Sie fließend Deutsch? – zulässig, wenn für die angebotene Tätigkeit erforderlich	Kann in anderen Fällen auf mittelbare Diskriminierung wegen der ethnischen Zugehörigkeit hindeuten.
Ausbildung und Berufserfahrung	Grundsätzlich zulässig	Unzulässig, wenn nach Ausbildung oder Berufserfahrung gefragt wird, die nicht tätigkeitsrelevant ist – Hinweis auf mögliche Diskriminierung wegen der ethnischen Zugehörigkeit
Vorstrafen	Sind Sie je wegen eines Vergehens/ Verbrechens verurteilt oder angeklagt worden?	Stets unzulässig ist es, nach Anklagen zu fragen, die nicht in Verurteilung mündeten. Im Übrigen wie in Deutschland nur tätigkeitsbezogen – ansonsten Hinweis auf mittelbare Diskriminierung wegen der ethnischen Zugehörigkeit (wegen der prozentual deutlich höheren Vorstrafen-Quote Farbiger in den USA
Mitgliedschaften		Listen Sie alle Vereins-, Club- oder sonstige Mitgliedschaften auf – mittelbare Rassendiskriminierung

[Entnommen aus: Thüsing, Arbeitnehmerdatenschutz und Compliance (Beck, 2010), S. 187 f.]

1. Einstellung: Fragerecht und Datennutzung

"Erledigte Ermittlungsverfahren„ BAG, Urteil v. 15.11.2012 - 6 AZR 339/11

Leitsatz

An der Informationsbeschaffung durch die unspezifizierte Frage nach eingestellten Ermittlungsverfahren an den Stellenbewerber besteht grundsätzlich kein berechtigtes Interesse des potenziellen Arbeitgebers.

Eine solche Frage ist damit im Regelfall nicht erforderlich iSv. § 29 Abs. 1 Satz 1 DSG NRW. Das ergibt sich aus den Wertentscheidungen des § 53 BZRG.

Eine allein auf die wahrheitswidrige Beantwortung einer solchen Frage gestützte Kündigung verstößt deshalb gegen die objektive Wertordnung des Grundgesetzes, wie sie im Recht auf informationelle Selbstbestimmung zum Ausdruck kommt, und ist nach § 138 Abs. 1 BGB unwirksam.

Orientierungssätze

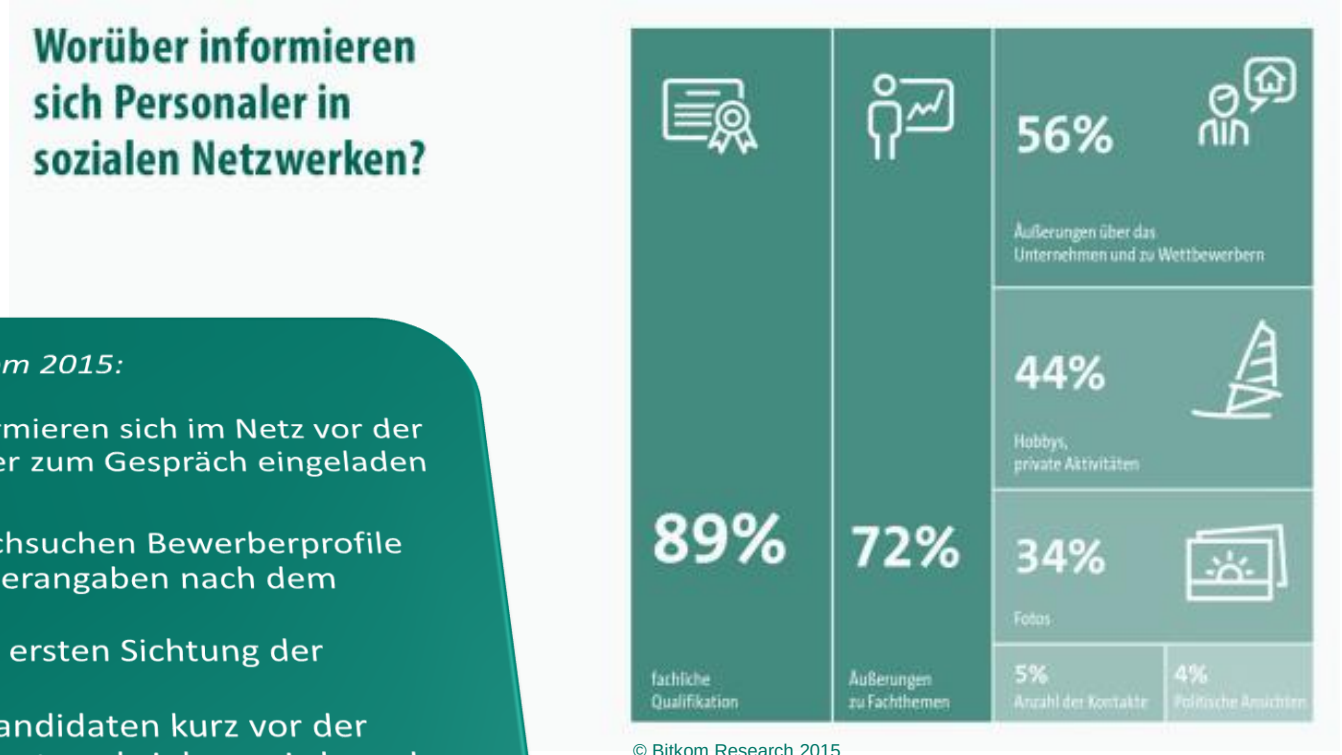
Vom Schutzzweck des § 612a BGB wird nicht der Fall der Rechtsausübung vor Begründung des Arbeitsverhältnisses, welche erst im späteren Arbeitsverhältnis zu Nachteilen führt, erfasst.

Fragen nach personenbezogenen Daten vor der Eingehung eines Arbeitsverhältnisses sind dann […] erforderlich, wenn der künftige Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse an der Beantwortung seiner Frage beziehungsweise der Informationsbeschaffung im Hinblick auf die Begründung des Arbeitsverhältnisses hat und das Interesse des Arbeitnehmers an der Geheimhaltung seiner Daten das Interesse des Arbeitgebers an der Erhebung dieser Daten nicht überwiegt.

1. Fragerecht und Datennutzung: „Ungefragt“ erhobene Daten

Repräsentative Umfrage Bitkom 2015:

- *62 % der Unternehmen informieren sich im Netz vor der Entscheidung, ob ein Bewerber zum Gespräch eingeladen wird*
- *46% Chefs & Personaler durchsuchen Bewerberprofile*
- *39 % überprüfen die Bewerberangaben nach dem Gespräch*
- *30 % tun dies bereits bei der ersten Sichtung der Unterlagen*
- *12 % gleichen ihr Bild vom Kandidaten kurz vor der Entscheidung, ob ein Vertrag unterschrieben wird, noch einmal mit den Social-Media-Profilen ab*



© Bitkom Research 2015

2. Personalakte

Personalakte im materiellen Sinn: Jede Sammlung von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse des Arbeitnehmers betreffen und in einem inneren Zusammenhang mit dem Arbeitsverhältnis stehen.	**Zweck:** Vermittlung eines möglichst vollständigen, wahrheitsgemäßen und sorgfältigen Bildes über die persönlichen und dienstlichen Verhältnisse des Arbeitnehmers
	Grundsätze: Vertraulichkeit, Vollständigkeit und Richtigkeit
	Zulässige Inhalte sind an § 32 Abs. 1 S. 1 i.V.m. **§ 32 Abs. 2 BDSG** zu messen
	AN-Rechte: Einsichtnahme, Abgabe von Erklärungen, Entfernungsanspruch
	Auf **in Papierform geführte Personalakten** finden die §§ 33, 34, 35 BDSG grds. keine Anwendung. Anders aber, wenn es sich bei der manuell geführten Personalakte um eine nicht automatisierte Datei i.S.d. § 3 Abs. 2 Satz 2 BDSG handelt = BDSG gilt für gleichförmig strukturierte, manuell auswertbar geführte Aktenbestände mit personenbezogenen Daten, wie etwa Personalkarteien.
	Keine Aufbewahrungspflicht bezgl. Personalakten ausgeschiedener Arbeitnehmer soweit nicht Sondervorschriften greifen (z.B. § 41 Abs. 1 Nr. 9 EStG für Lohnkonten).
	Ratsam: Personalakte jedenfalls für die Dauer noch laufender Verjährungs- und Ausschlußfristen aufbewahren.

3. Elektronischer Datenabgleich / Screening

Am Beispiel der Anfang 2009 bekannt gewordenen Vorgänge bei der Deutschen Bahn AG:

Maschinelles Screening = automatisierte Verarbeitung i.S.d. § 3 Abs. 2 BDSG

Compliancepflicht vs. PersönlichkeitsR

Datenerhebung

Angaben, die dem Unternehmen gegenüber gemacht wurden, z.B. Personal- & Kreditoren-Stammdaten

Datenabgleich

Überprüfung von Übereinstimmungen

Datenscreening

= Abgleich von internen und externen Datenbeständen

Rechtmässigkeit Erhebung?

- § 28 I S.1 Nrn. 1 – 3 BDSG
- AN: § 32 I S. 1 BDSG

Aber: Zweckbestimmung!

[P]: Einwilligung / Information bzgl. weitergehender Nutzung (-)

Rechtmässigkeit Nutzung?

- § 28 II BDSG: Abwägung!
- AN: § 32 I S. 2 BDSG: Tatsächliche Anhaltspunkte Erforderlichkeit Verhältnismäßigkeit

4. E-Mail & **Internet**

Grenze
der Zulässigkeit:

Keine lückenlose und detaillierte Überwachung des Nutzungsverhaltens!

-> Verdachtsbezogene stichprobenartige Log-File-Kontrolle ist ein geeignetes milderes Mittel

MBR!
§ 87 Abs.1 Nr. 6 BetrVG

Vielfältige technische Überwachungsinstrumente:

- ✓ Firewall
- ✓ Logfiles, Browser-Historie, Überwachungssoftware
- ✓ Spezielle Hardware-Komponenten

Kontrolle der äußeren Verbindungs-daten („Monitoring“) stets zulässig	Berechtigtes AG-Interesse überwiegt. AN muß jedoch vorab informiert sein!
	Erfassung IP-Adresse des benutzten Rechners sowie sämtlicher Daten, die sich auf die Dienstnutzung beziehen: Art, Umfang des Datenverkehrs, Zeiten sowie URL der aufgerufenen Webseiten

1. Ausnahme: AN mit Sonderstatus
- Berufsgruppen des § 203 StGB
- Journalisten, Geistliche, Richter, wissenschaftlich tätige Personen

2. Ausnahme: Interessenvertretungen
- Schutz der Aufgabenwahrnehmung überwiegt grds. AG-Interesse

Hier **Überwachung** und Kenntnisnahme der Kommunikationsinhalte grundsätzlich **unzulässig**!

4. **E-Mail** & **Internet**

Auch bei ausschließlich dienstlicher Nutzung kein Recht des AG auf Kenntnisnahme von ausdrücklich als privat gekennzeichnetem oder erkennbaren Inhalten!

Aber: Sofern nicht ausdrückliche gekennzeichnet oder als persönlich oder vertraulich erkennbar, darf nach h.M. bei ausschließlich dienstlicher Gestattung auch E-Mail gelesen werden, die an eine persönliche Adresse (z.b. „strunk@hsv-fl.de) gesendet wurde!

Handhabungsmöglichkeit für Trennung von aufbewahrten Inhalten in der Praxis:

Kennzeichnung von Ordnern

- Kontrolle der **Verbindungsdaten** stets zulässig
  Außer den Übertragungsdaten auch Infos im E-Mail-Header (Absender, Betreff etc.) = zulässiger Eingriff in GR des AN
- **Automatisierte Kontrolle** durch Virencheck stets zulässig
  Auch: Unterdrückung von Teilinhalten oder Anlagen von Nachrichten, die gefährlichen oder verdächtigen Code bzw. Dateierweiterungen beinhalten
- **[P] E-Mail-Adresse des Empfängers**: Nach h.M. zulässig
  Arg.: Parallele zur schriftlichen dienstlichen Kommunikation
- **[P] Kenntnisnahme des E-Mail-Inhalts**: Sehr umstritten!
  „Gretchenfrage“: Ist E-Mail-Kommunikation eher mit Telefonat oder eher mit herkömmlichem Schriftverkehr zu vergleichen?
  - Ablehnende Ansicht: Grds. kein Zugriff des AG auf die Inhalte dienstlicher E-Mails, da Charakter eines Telefonats. Insbesondere Empfänger rechnet nicht damit, daß noch andere mitlesen.
  - Befürworter: Schriftliche Äußerung, daher keine „Flüchtigkeit“ und kein Schutzbedürfnis wg. Korrigierbarkeit wie beim Telefonat.

  Jedenfalls: Mitarbeiter müssen über Zugriffsbefugnis informiert sein, sonst besondere Rechtfertigung im Einzelfall erforderlich!

5. Telefon

§ 88 TKG

- Mithören – egal ob offen oder heimlich – und Aufzeichnen von Telefonaten grds. unzulässig
- Kommunikationsinhalte über §206 V S.2 StGB geschützt -> § 206 I StGB
- Vertraulichkeit des nicht öff. gespr. Wortes -> § 201 StGB

Einwilligung gem. §§ 4a, 4 Abs. 1 BDSG möglich, jedoch hohe Anforderungen an Wirksamkeit

Erlaubte Privatnutzung

Rein dienstliche Nutzung

Immer noch relevant - der Klassiker:

Arbeitgeber = TK-Anbieter

i.S.d. § 3 Nr. 6 TKG?

(+) = h.M.

(-) = Teile Lit. & Rechtsprechung

(LAG Berlin-Brandenburg, 16.02.2011 - 4 Sa 2132/10; LAG Niedersachsen, 31.05.2010 - 12 Sa 875/09; VG Karlsruhe, 27.05.2013 – 2 K 3249/12 „Mappus“)

Aber: Besondere Situation BYOD!

BDSG

- Mithören – egal ob offen oder heimlich – und Aufzeichnen von Telefonaten grds. unzulässig
- § **201 StGB** bei Aufzeichnung
- § **32 Abs. 1 S. 1 BDSG?** Regelmäßig (-), für **offenes** Mithören und Aufzeichnen in Call-Center denkbar (z.B. Beweiszwecke; str.: Schulungszwecke – hier ggf. Einwilligung einholen)
- § **32 Abs. 1 S. 2 BDSG?** Absoluter Ausnahmefall: Erhebliche Auswirkungen für ArbV, nur partiell zulässig.

Sonderfall: „Angekündigtes heimliches Mithören“ im Call-Center
[P] Legitimation durch § 32 I 1 BDSG?
-> Bislang keine Rechtsprechung = Einwilligung einh.

MBR!
§ 87 Abs.1 Nr. 6 BetrVG

Exkurs: BYOD

Einbindung privater („fremder“) Endgeräte in die IT-Infrastruktur des Unternehmens

In aller Regel **personenbezogene Daten betroffen**: Kontaktdaten und weitere Angaben zu Kollegen, Kunden, Interessenten und sonstigen Geschäftspartnern

Verarbeitung personenbezogener betriebsbezogener Daten mit privaten Geräten zulässig, allerdings **BDSG einzuhalten**, da § 1 Abs. 2 Nr. 3 BDSG (-): Erhebung, Verarbeitung und Nutzung von Daten erfolgt dann nicht „ausschließlich für persönliche oder familiäre Tätigkeiten“.

Arbeitnehmer wird nicht zur verantwortlichen Stelle, § 3 Abs. 7 BDSG. Tätigkeit erfolgt in Erfüllung seiner Pflichten aus dem Arbeitsverhältnis und damit für den Arbeitgeber.

Arbeitgeber = TK-Anbieter
i.S.d. § 3 Nr. 6 TKG?

Arbeitgeber daher für die Einhaltung der datenschutzrechtlichen Vorschriften im Hinblick auf diejenigen Daten **verantwortlich**, die durch ihre Arbeitnehmer auf deren privaten Endgeräten verarbeitet werden

Insbesondere Sicherstellung technische & organisatorische Maßnahmen („TOM“) gem. **§ 9 BDSG**

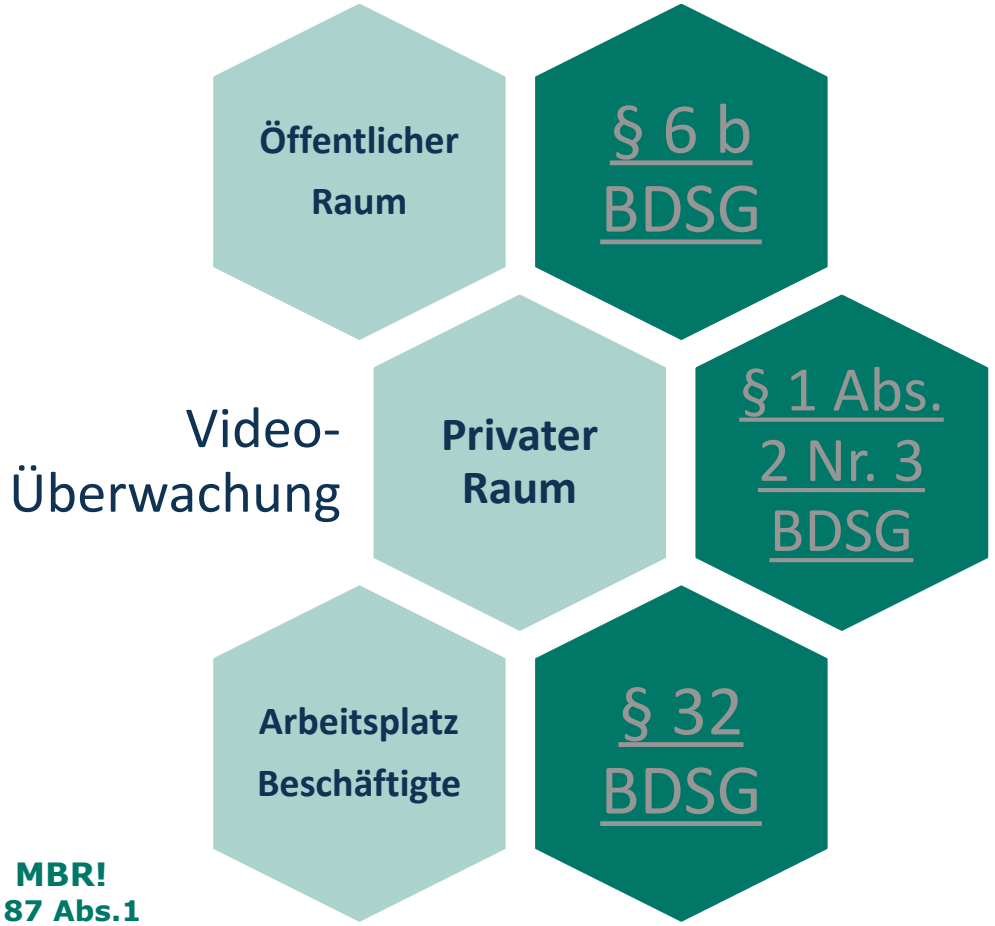
Zunächst Risikoanalyse: Welche Daten werden einem Zugriff durch private Endgeräte von Arbeitnehmern zugänglich gemacht,

dann Bestimmung der erforderlichen Maßnahmen gem. § 9 BDSG, z.B.: „Container“-Apps (Trennung von Inhalten), Unternehmenszugriff auf Endgerät durch Device Management-Programme (Fernzugriff)

Transparente Information der Arbeitnehmer über Voraussetzungen und Bedingungen der Nutzung privater Endgeräte:

Wirksamkeitserfordernis für informierte Einwilligung, § 4 Abs. 3 BDSG in die Kontrolle des BYOD-Einsatzes durch das Unternehmen.

6. Video-Überwachung



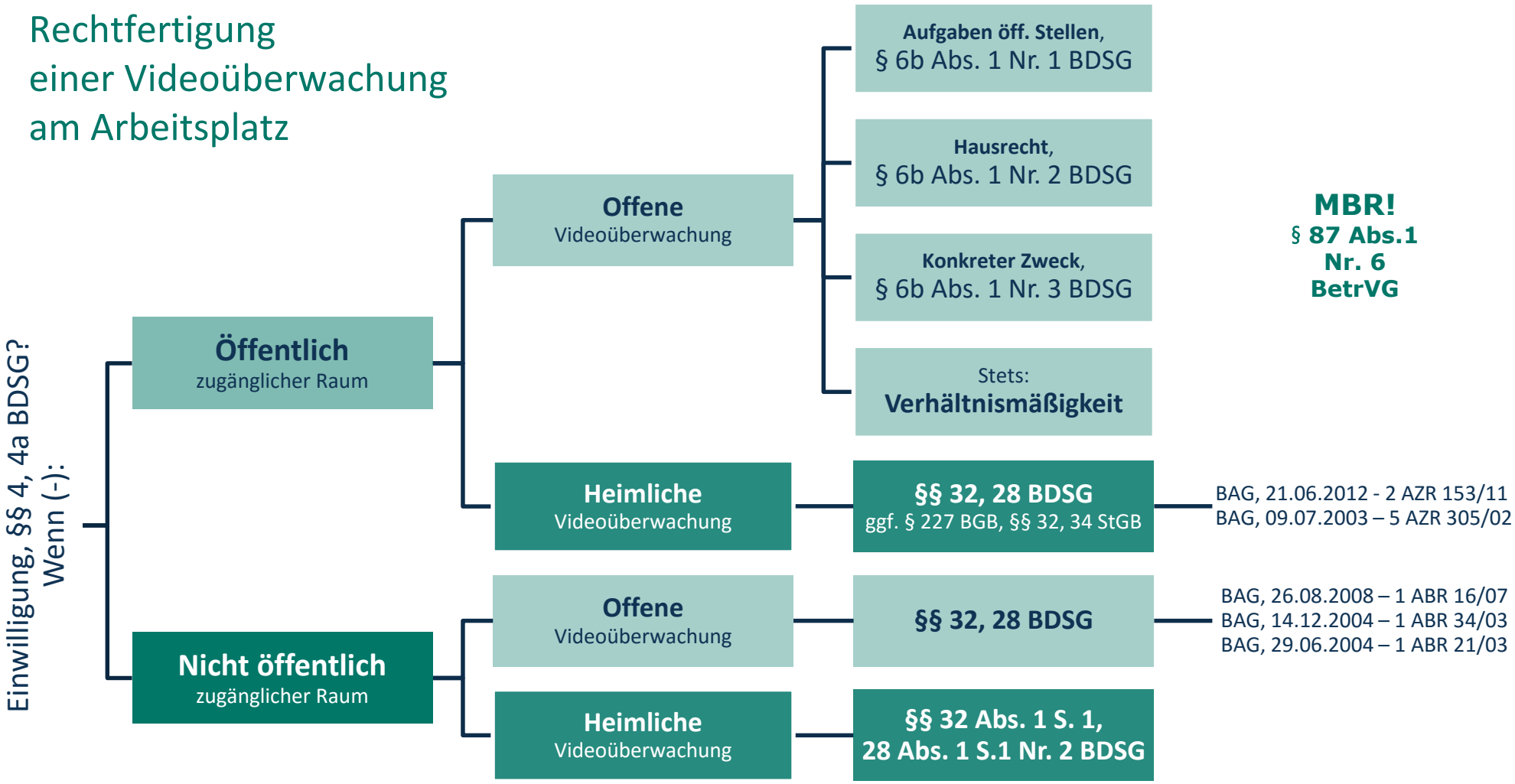
MBR!
§ 87 Abs.1 Nr. 6 BetrVG

- **[P] Verhältnis § 6 b - § 32 BDSG:**

1. Erfassung von Kunden / Lieferanten und gleichzeitig MA auf Betriebsgrundstück -> Vermittelnde Ansicht: Parallele Anwendung mit angemessener Einschränkung im Einzelfall
2. **Nicht öffentliche Betriebsräume**: Str., ob strenger Maßstab ÖR (*so BAG, Urt. v. 29.06.2004 – 1 ABR 21/03*), da sich der AN der Überwachung nicht entziehen könne) oder ausschließlich Maßstab des § 32 BDSG gilt , da kein erhöhter Überwachungsdruck (*so aktuell BAG, Urt. v. 21.06.2012 – 2 AZR 153/11*).

- **Regelung per BV** (§ 87 Abs. 1 Nr. 6 BetrVG) **zulässig**, aber Begrenzung durch Verhältnismäßigkeitsprinzip

Rechtfertigung einer Videoüberwachung am Arbeitsplatz



"Verdeckte Videoüberwachung„: Beweisverwertungsverbot bei Verstoß gg. § 32 BDSG?

-> BAG, Urteil v. 21.06.2012 - 2 AZR 153/11 = Hier noch ausdrücklich offen gelassen, da ÜW vor Novelle erfolgte

Leitsätze:

(1) Entwendet eine Verkäuferin Zigarettenpackungen aus dem Warenbestand des Arbeitgebers, kann dies auch nach längerer Beschäftigungsdauer eine Kündigung des Arbeitsverhältnisses rechtfertigen.

(2) Das aus einer verdeckten Videoüberwachung öffentlich zugänglicher Arbeitsplätze gewonnene Beweismaterial unterliegt nicht allein deshalb einem prozessualen Beweisverwertungsverbot, weil es unter Verstoß gegen das Gebot in § 6b Abs. 2 BDSG gewonnen wurde, bei Videoaufzeichnungen öffentlich zugänglicher Räume den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen kenntlich zu machen.

Orientierungssätze:

1. Für den Grad des Verschuldens und die Möglichkeit einer Wiederherstellung des Vertrauens macht es objektiv einen Unterschied, ob es sich bei einer Pflichtverletzung um ein Verhalten handelt, das insgesamt auf Heimlichkeit angelegt ist oder nicht.

2. Bei der Abwägung zwischen dem Interesse an einer funktionstüchtigen Rechtspflege und dem Schutz des informationellen Selbstbestimmungsrechts als Ausfluss des allgemeinen Persönlichkeitsrechts hat das Interesse an der Verwertung der einschlägigen Daten und Erkenntnisse nur dann höheres Gewicht, wenn weitere, über das schlichte Beweisinteresse hinausgehende Aspekte hinzukommen, die ergeben, dass das Verwertungsinteresse trotz der Persönlichkeitsbeeinträchtigung überwiegt. Allein das Interesse, sich ein Beweismittel zu sichern, reicht nicht aus. Die weiteren Aspekte müssen gerade eine bestimmte Informationsbeschaffung und Beweiserhebung als schutzbedürftig qualifizieren.

3. Die heimliche Videoüberwachung eines Arbeitnehmers ist zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit praktisch das einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist. Der Verdacht muss in Bezug auf eine konkrete strafbare Handlung oder andere schwere Verfehlung zu Lasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern bestehen.

4. Auch im Hinblick auf die Möglichkeit einer weiteren Einschränkung des Kreises der Verdächtigen müssen weniger einschneidende Mittel als eine verdeckte Videoüberwachung zuvor ausgeschöpft worden sein.

Schmerzensgeldanspruch des AN bei rechtswidrigen heimlichen Videoaufnahmen

-> BAG, Urteil v. 19.02.2015 - 8 AZR 1007/13

„Durch Privatdetektive erhobene Daten, die bestimmte oder bestimmbare natürliche Personen betreffen, sind personenbezogene Daten iSv. § 32 Abs. 1 Satz 2 BDSG. […].
Ihre Erhebung, Aufbewahrung und Übermittlung durch einen Auftraggeber oder durch Privatdetektive, die auf eigene Rechnung handeln, ist eine „Verarbeitung personenbezogener Daten. […].
Auch das von einer Kamera aufgezeichnete Bild einer Person fällt unter den Begriff der personenbezogenen Daten, sofern es die Identifikation der betroffenen Person ermöglicht."

Kernaussagen:	Ein Arbeitgeber, der wegen des Verdachts einer vorgetäuschten Arbeitsunfähigkeit einem Detektiv die Überwachung eines Arbeitnehmers überträgt, handelt rechtswidrig, wenn sein Verdacht nicht auf konkreten Tatsachen beruht.
	In einer unzulässigen Observation liegt eine Verletzung des APR des Betroffenen, die durch heimlich hergestellte Video-Aufnahmen intensiviert wird.
	Eine solche rechtswidrige Verletzung des allgemeinen Persönlichkeitsrechts kann einen Geldentschädigungsanspruch („Schmerzensgeld") begründen.

6. Video-Überwachung

Beeinträchtigung des Allgemeinen Persönlichkeits-rechts durch Kamera-Attrappe?

Landgericht Bonn, Urt. v. 16.11.2004 - 8 S 139/04:

„Die Beseitigung einer auf das Nachbargrundstück gerichteten Kamera kann auch dann verlangt werden, wenn damit keine Videoaufnahmen gefertigt werden bzw. gefertigt werden können, da der beim Nachbarn erzeugte "Überwachungsdruck" einen Eingriff in das allgemeine Persönlichkeitsrecht begründet.“

Amtsgericht Schöneberg, Urt. v. 30.07.2014 - 103 C 160/14:

„Lässt der Vermieter im Eingangsbereich des Hauses Geräte, die wie Videokameras aussehen, bei denen es sich jedoch um Attrappen handelt, die Aufnahmen nicht herstellen können, deswegen anbringen, um nach Möglichkeit Vandalismusschäden im Hauseingangsbereich durch außenstehende Personen zu vermeiden, liegt eine Verletzung des allgemeinen Persönlichkeitsrechts der Mieter nicht vor.

Allein die Befürchtung des Mieters, der Vermieter könnte eines Tages die Attrappen durch echte Kameras auswechseln, begründet noch keinen Eingriff in das allgemeine Persönlichkeitsrecht des Mieters“

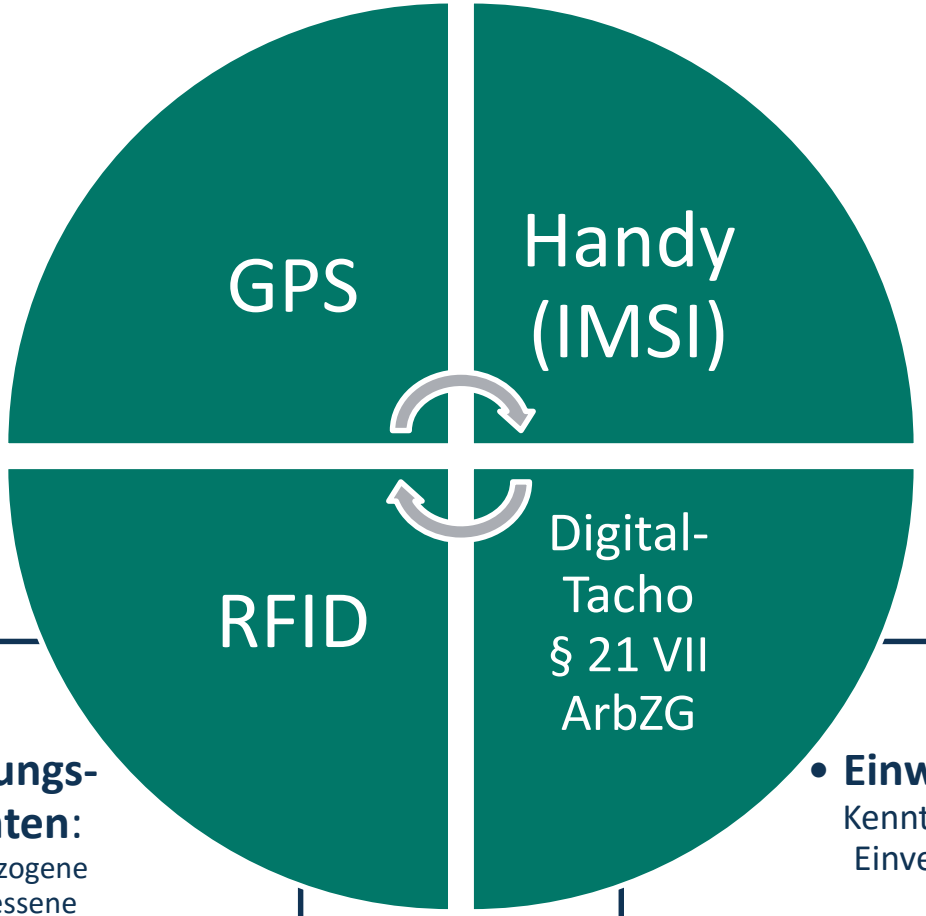
MBR des Betriebsrats bei Installation einer Kamera-Attrappe durch AG?

LAG Rostock *(Beschluss vom 12.11.2014 - 3 TaBV 5/14)*

7. GPS-Ortung

Privatbereich
Ortung nie zulässig, da § 32 Abs. 1 BDSG (auch § 28 Abs. 1 S. 1 Nr. 2) konkreten Zusammenhang mit dem Arbeitsverhältnis erfordern.

[P] Privat genutztes Dienstfahrzeug:
Keine Ortung außerhalb der Arbeitszeit



Dienstliche Tätigkeit
Zwecke:
- Sicherheit AN & Betriebsmittel
- Einsatzkoordination
- Diebstahlsicherung
- Sendungsverfolgung
- Aufdeckung von Verstößen

Zulässigkeitsmaßstab:
- § 32 Abs. 1 S. 1
- § 28 Abs. 1 S. 1 Nr. 2
- § 32 Abs. 1 S. 2
- § 28 Abs. 2 Nr. 2

[P] Heimlichkeit

MBR!
§ 87 Abs.1 Nr. 6 BetrVG

- **Löschungs-Pflichten**:
  Anlaßbezogene angemessene Aufbewahrungsdaer

- **Einwilligung:**
  Kenntnis ist kein Einverständnis!

Vorsätzliches unbefugtes Erheben von Daten: "GPS-Sender"

-> BGH, Urteil v. 04.06.2013 - - 1 StR 32/13

Grund-aussagen:

Das Sammeln von minütlich oder alle zwei Minuten in geografischen Breiten- und Längenkoordinaten ausgedrückten Positionsdaten der GPS-Empfänger mittels der GPS-Empfänger ist eine Datenerhebung im Sinne des § 3 Abs. 3 BDSG.

Soweit diese Daten computergestützt mittels Software automatisch zu Bewegungsprotokollen zusammengefügt werden, liegt zudem eine automatisierte Weiterverarbeitung im Sinne des § 3 Abs. 4 Satz 2 Nr. 2 BDSG vor.

Allgemein zugänglich sind nur Daten, die von jedermann zur Kenntnis genommen werden können, ohne dass der Zugang zu den Daten rechtlich beschränkt ist. Rechtliche Schranken jedweder Art des Zugangs zu den Daten, auch wenn die rechtlichen Hürden nicht besonders hoch sind und mittels Falschangaben einfach umgangen werden können, schließen die allgemeine Zugänglichkeit aus.

Unbefugtes Handeln im Sinne des § 43 Abs. 2 Nr. 1 BDSG liegt vor, wenn nicht Rechtssätze das Verhalten erlauben. Als spezifische datenschutzrechtliche Erlaubnisse kommen § 28 BDSG oder § 29 BDSG in Betracht.

Beide grundsätzlich in Betracht kommende Erlaubnissätze müssen im Hinblick auf die Voraussetzungen einer Befugnis zum Umgang mit „fremden“ personenbezogenen Daten anhand der europäischen Datenschutzrichtlinie ausgelegt werden. Die Zulässigkeit der Datenverarbeitung erfordert daher zum einen, dass die Verarbeitung personenbezogener Daten zur Verwirklichung des von dem Überwachenden oder dessen Auftraggeber wahrgenommenen berechtigten Interesses erforderlich ist, und zum anderen, dass die Grundrechte und Grundfreiheiten der von der Observation betroffenen Person nicht überwiegen.

Stammen die verarbeiteten Daten aus nicht öffentlich zugänglichen Quellen, ist zu berücksichtigen, dass der Überwachende und sein Auftraggeber zwangsläufig Informationen über die Privatsphäre der betroffenen Person erlangen. Diese schwerwiegendere Beeinträchtigung der verbürgten Rechte der betroffenen Person ist zu berücksichtigen, indem sie gegen das berechtigte Interesse an der Überwachung im Einzelfall abgewogen wird. Dies bedeutet, dass sämtliche Rechtspositionen des von der Observation Betroffenen, die der Privatsphäre zuzuordnen sind, zu gewichten und in die Abwägung einzustellen sind.

Ob die Interessen des Betroffenen am Schutz seiner Privatsphäre und seiner personenbezogenen Daten überwiegen, ist eine Frage des Einzelfalls, die durch den Tatrichter zu beantworten ist.

„Ältere“ Rechtsprechung zur technischen Überwachung:

ArbG Düsseldorf

- Außerordentliche Kündigung eines Arbeitnehmers wegen Unterschlagung (Verwertbarkeit heimlicher Videoaufnahmen)
  Urteil v. 03.05.2011 – Az. 11 Ca 7326/10

LAG Köln

- Außerordentliche Kündigung einer Kassenangestellten (Verwertbarkeit heimlicher Videoaufnahmen)
  Urteil v. 18.11.2010 – Az. 6 Sa 817/10

LAG Köln

- Außerordentliche Kündigung eines Schwerbehinderten wg. heimlichen Aufzeichnens von Personalgesprächen
  Urteil v. 18.05.2011 – Az. 8 Sa 364/2011

LAG Berlin-Brandenburg

- Unterlassungsklage wegen Zugriff des Arbeitgebers auf dienstlichen E-Mail-Account einer abwesenden Mitarbeiterin
  Urteil v. 16.02.2011 – Az. 4 Sa 2132/10

Standort

I. Gesetzliche Grundlagen und Systematik des AN-Datenschutzes
II. Typische Konfliktfelder im Unternehmen
III. Datentransfer im Konzern und Zulässigkeit der Weitergabe von AN-Daten an Dritte
IV. Betriebsverfassungsrechtliche Rahmenbedingungen der Datenverarbeitung
V. Informations-/Handlungspflichten des Arbeitgebers
VI. Rechtsfolgen bei Verstößen

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

Datentransfer im und aus dem Unternehmen

Innerhalb des Unternehmens
(z.B. Revisons-, Complianceabteilung, Zentralrechner)

Externe Stellen
(z.B. Outsourcing an Drittdienstleister, due-diligence-Prüfung)

Weitergabe personenbezogener Daten
von Mitarbeitern *(= § 32 BDSG)* oder Firmenfremden *(= § 28 BDSG)*

unter Beteiligung
einer *(= Nutzung)* oder
mehrerer *(=Übermittlung)* Stellen

Inland

Ausland

Exkurs: Arbeitnehmer-Daten & MiLoG

Keine Beschäftigtendaten für Auftraggeber nötig zum Nachweis der Mindestlohnzahlung	Mit dem Mindestlohngesetz sind Unternehmer gehalten, ihren Beschäftigten den gesetzlichen Mindestlohn zu zahlen. Für die Einhaltung dieser Verpflichtung haften verschuldensunabhängig auch Auftraggeber, die andere Unternehmen mit der Erbringung von Dienst- oder Werkleistungen betrauen. Zur Begrenzung des Haftungsrisikos ist der Auftraggeber gehalten, geeignete Maßnahmen zu ergreifen. **Hierfür ist es weder nötig noch datenschutzrechtlich zulässig, sensible Beschäftigtendaten pauschal an Auftraggeber weiterzugeben**. […].
	Beauftragte Unternehmer und Subunternehmer müssen im Einzelfall prüfen, inwieweit sie ihre Beschäftigtendaten an den Auftraggeber übermitteln dürfen. Spiegelbildlich betrachtet muss ein Auftraggeber untersuchen, ob ihm für Daten eine gesetzliche Erhebungsbefugnis zusteht. Die Auftraggeber müssen ihre zu beauftragenden Unternehmer sorgfältig auswählen. Regelmäßig ergeben sich schon aus einem Angebot Indizien dafür, dass keine Mindestlöhne bezahlt werden.
	[…]. **Ein Auftraggeber (muss) alle Möglichkeiten ausschöpfen, ohne zuordenbare Beschäftigtendaten sein Haftungsrisiko zu verringern**. Dem dienen vertragliche Zusicherungen von den Unternehmern und Subunternehmern, Vertragsstrafenregelungen und Bankbürgschaften. **Die Übersendung von nicht anonymisierten Gehaltsbescheinigungen an den Auftraggeber sowie die pauschale Einräumung von Einsichtsrechten in Personalaktenbestandteile der beauftragten Unternehmer und Subunternehmer sind unzulässig.**

[Quelle: Pressemitteilung vom 06.02.2015 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein]

Sonderfall: **Auftragsdatenverarbeitung** (ADV)

= Auslagerung von Daten an Auftragnehmer innerhalb EU

= Keine Übermittlung von Daten i.S.d. BDSG

h.M. (DS-Behörden):

„Funktions-übertragungs-lehre“

Übermittlung von Daten i.S.d. BDSG

Auftragsdatenverarbeitung

§ 11 BDSG

- DV ist Vertragsschwerpunkt, Zugriff AuN
- Keine eigenen Entscheidungsbefugnisse des AuN über Verwendung von Daten
- Reine Infrastrukturnutzung durch AuG

Auftragnehmer = Tätigkeit nur nach Weisung, AG bleibt verantwortliche Stelle i.S.d. BDSG

[P] Abgrenzung!

Funktionsübertragung

§ 3 Abs. 4 Satz 2 Nr. 3 BDSG

- Nutzung für eigene Zwecke
- Dienstleistung geht über rein techn. / organisatorische Bereitstellung hinaus
- fehlender Einfluß des Auftraggebers

Dritter = eigenverantwortlich tätiger Datenverarbeiter

Anforderungen: § 11 Abs. 2 i.V.m. § 9 BDSG

Prüfungsübersicht: Grenzüberschreitender Datenverkehr

1. Stufe:

Normale Zulässigkeitsprüfung für Übermittlung personenbezogener Daten an Dritten

2. Stufe:

Ist die **grenzüberschreitende Übermittlung** zulässig?

Maßstab: § 4b BDSG, § 4c BDSG

EU- oder EWR-Land	Sonstiges Land mit „angemessenem Schutzniveau“	Ausnahme gem. § 4c BDSG liegt vor (z.B. Einwilligung)	Drittstaat ohne angemessenes Schutzniveau (z.B. USA, Rußland)
Übermittlung zulässig			**Übermittlung verboten**

„Rettungsanker“:

- **Safe Harbor für die USA aktuell weggefallen!**
- **§ 4 c BDSG**

6.10.2015: EuGH zu Safe Harbor (Schrems ./. Data Protection Commissioner (C 362/14)

Die Richtlinie 95/46 ist dahin auszulegen, dass eine aufgrund dieser Bestimmung ergangene Entscheidung […] die feststellt, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine Kontrollstelle eines Mitgliedstaats […] nicht daran hindert, die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten.

In der Entscheidung 2000/520 wird den „Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen“ Vorrang vor den Grundsätzen des „sicheren Hafens“ eingeräumt; aufgrund dieses Vorrangs sind die selbstzertifizierten US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne jede Einschränkung verpflichtet, die Grundsätze des „sicheren Hafens“ unangewandt zu lassen, wenn sie in Widerstreit zu den genannten Erfordernissen stehen […].

Der Erlass einer Entscheidung der Kommission erfordert[…], dass das betreffende Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Grundrechte gewährleistet, das dem in der Rechtsordnung der Union garantierten Niveau […] der Sache nach gleichwertig ist. Die Kommission hat jedoch in der Entscheidung 2000/520 nicht festgestellt, dass die Vereinigten Staaten von Amerika aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein angemessenes Schutzniveau „gewährleisten“. Daher ist, ohne dass es einer Prüfung des Inhalts der Grundsätze des „sicheren Hafens“ bedarf, der Schluss zu ziehen, dass Art. 1 der Entscheidung 2000/520 gegen die in […] der Richtlinie 95/46 […] festgelegten Anforderungen verstößt und aus diesem Grund ungültig ist.

Der sichere Hafen ist erst mal weg – was tun?

- Zur Erfüllung eines Vertrags zwingend erforderlich
- Übermittlung dient dem Interesse des Betroffenen

Gesetzliche Ausnahmen:

§ 4c Abs. 1 Nrn. 2-5 BDSG

Einwilligung

§ 4c Abs. 1 Nr. 1 BDSG

[P]
– Informierte Einwilligung, § 4a BDSG
- Zweckbindung, § 4 Abs. 3 BDSG

[P]
– Unveränderte Übernahme, sonst Gen. Aufsichtsbeh. erf.
- Datenimporteur muß sich d. DS-Aufsicht des Datenexporteurs unterwerfen

EU-Standard-Vertragsklauseln

§ 4c Abs. 2 BDSG

Binding Corporate Rules (BCR)

§ 4c Abs. 2 BDSG

[P]
– Gesamter Konzern unterliegt faktisch EU-DS-Recht
- Zustimmung aller DS-Behörden notwendig, in denen Konzernteile ihren Sitz haben

Aktuelle Stellungnahme *„Artikel-29-Gruppe"* vom 16.10.2015: „Galgenfrist" bis Ende Januar 2016 – danach Maßnahmen der Datenschutzaufsichtsbehörden – bei etw. Beschwerden aber ggf. auch früher

Standort

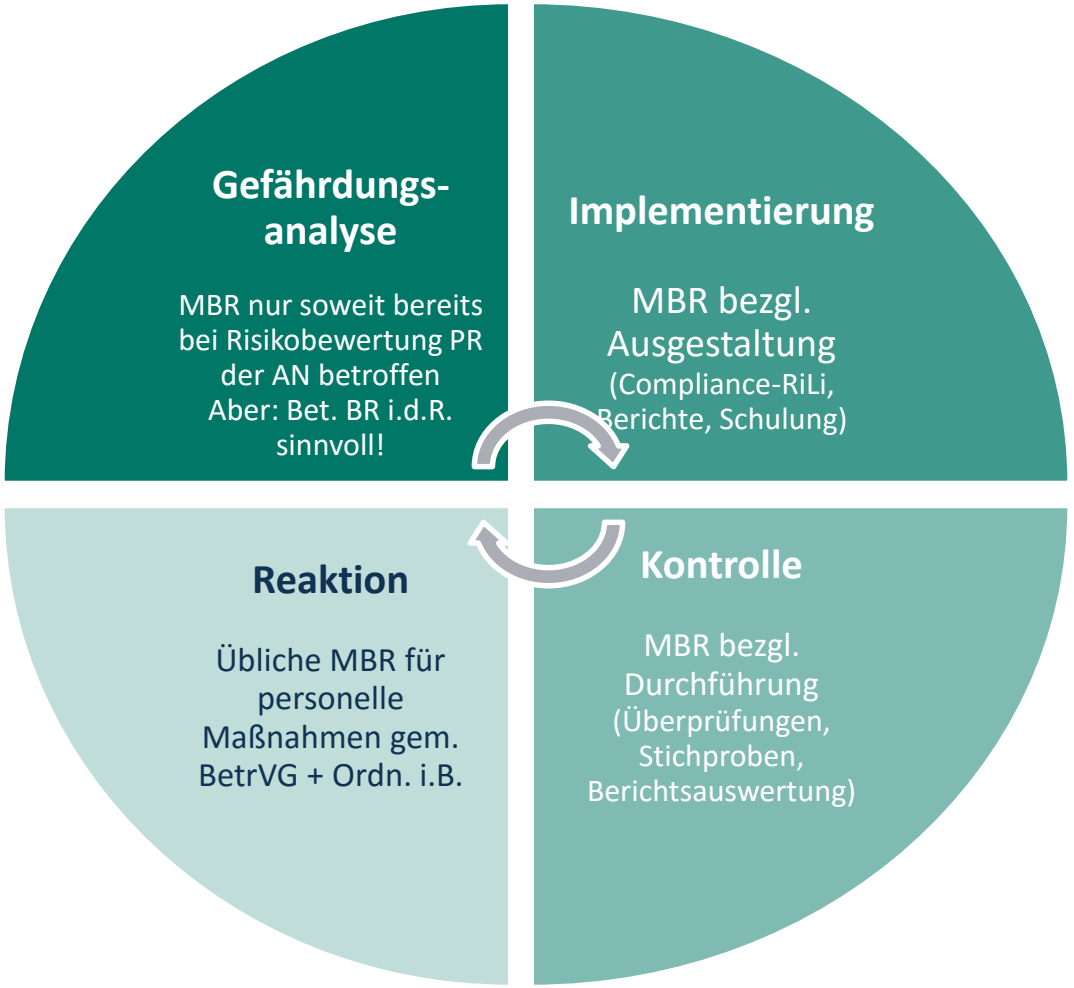
VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

Betriebsrat und Arbeitnehmerdatenschutz

Regelungsbedürftig:
Typische Konflikt-Bereiche im Unternehmen

MBR!
§ 87 Abs.1 Nr. 6 BetrVG

Compliance & Betriebsrat



Allgemeine **Beteiligungs**rechte des Betriebsrats

Mitwirkungsrechte des AN =
Unterrichtungs-/ Erörterungspflicht AG
+ Anhörungs- / Initiativrecht AN:

- § 81 Abs. 1 und 2 BetrVG: Unterrichtung
- § 81 Abs. 4 S.1 BetrVG: Unterrichtung
- § 81 Abs. 4 S.2 BetrVG: Erörterung
  (AN darf BR-Mitglied hinzuziehen, S. 3)
- § 82 Abs.1 BetrVG: Anhörung / Initiative

Mitwirkungsrechte: Betriebsrat / MAV

Inhalt der Bestimmung	**Betriebsverfassungsgesetz**	**MVG.EKD**
Schutz und Förderung der freien Entfaltung der Persönlichkeit der Arbeitnehmer	§ 75 Abs. 2 BetrVG	Keine gesetzliche Ausformulierung, da öffentliche Arbeitgeber und deren Belegschaftsvertretung ohnehin zur Einhaltung verpflichtet sind
Überwachung der Einhaltung der zugunsten der Arbeitnehmer bestehenden Datenschutzregelungen	§ 80 Abs. 1 Nr. 1 BetrVG	§ 35 Abs. 3 Buchst. b) MVG.EKD
Rechtzeitige und umfassende Unterrichtung zu geplanten IKT-Systemen	§ 80 Abs. 2 BetrVG	§ 34 Abs. 1 MVG.EKD
Mitbestimmung bei Leistungs- und Verhaltenskontrolle	§ 87 Abs. 1 Nr. 6 BetrVG	§ 40 Buchst. j) MVG.EKD
Festlegung der Verarbeitung personenbezogener Daten	-	-
Betriebs- oder Dienstvereinbarung	§ 77 BetrVG	§ 36 MVG.EKD

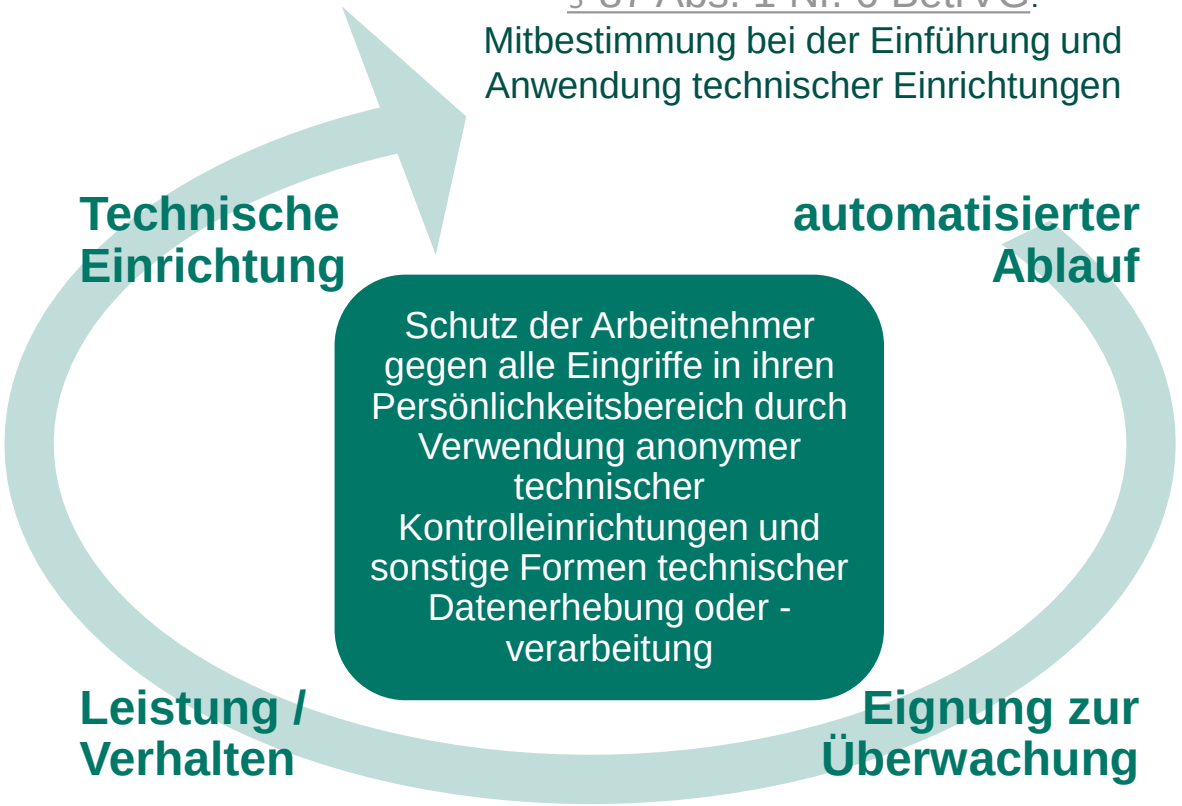
Mitwirkungsrechte: Personalrat

Inhalt der Bestimmung	**Bundespersonalvertretungsgesetz**	**Mitbestimmungsgesetz Schleswig-Holstein([MBG-SH)**
Schutz und Förderung der freien Entfaltung der Persönlichkeit der Arbeitnehmer	Keine gesetzliche Ausformulierung, da öffentliche Arbeitgeber und deren Belegschaftsvertretung ohnehin zur Einhaltung verpflichtet sind	Keine gesetzliche Ausformulierung, da öffentliche Arbeitgeber und deren Belegschaftsvertretung ohnehin zur Einhaltung verpflichtet sind
Überwachung der Einhaltung der zugunsten der Arbeitnehmer bestehenden Datenschutzregelungen	§ 68 Abs. 1 Nr. 2 BPersVG	"Allzuständigkeit" nach § 51 MBG-SH
Rechtzeitige und umfassende Unterrichtung zu geplanten IKT-Systemen	§ 68 Abs. 2 BPersVG	-
Mitbestimmung bei Leistungs- und Verhaltenskontrolle	§ 75 Abs. 3 Nr. 17 BPersVG	-
Festlegung der Verarbeitung personenbezogener Daten	-	§ 49 Abs. 1 MBG-SH
Betriebs- oder Dienstvereinbarung	§ 73 BPersVG	§ 57 MBG-SH

IKT-relevante Mitbestimmungsrechte des Betriebsrats

- § 87 Abs. 1 Nr. 7 BetrVG: Mitbestimmung in Fragen des Arbeits- und Gesundheitsschutzes
- § 91 Abs. 1 BetrVG: Mitbestimmung bei der Änderung von Arbeitsplätzen, Arbeitsabläufen oder –umgebungen

§ 87 Abs. 1 Nr. 6 BetrVG:
Mitbestimmung bei der Einführung und Anwendung technischer Einrichtungen



Mögliches [P]: Zuständiges Gremium (BR/GBR/Konzern-BR)
LAG Niedersachsen, Urt. v. 24.05.2011 – Az. 1 TaBV 55/09

Datenverarbeitung beim BR

Keine datenschutzrechtliche Selbständigkeit des BR!

[P]: Recht des BR auf Online-Zugriff auf DV-Verfahren beim Arbeitgeber?

Str.! Wohl (-), allenfalls durch BV regelbar

(Keine?) Kontrolle des BR durch den DSB

Der betriebliche Datenschutz-beauftragte	wirkt gem. § 4g Abs. 1 Nr. 1 BDSG auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hin
	ist gem. § 4g Abs. 1 Nr. 1 BDSG mit der Überwachung des datenschutzkonformen Umgangs mit den personenbezogenen Daten beauftragt.
	nimmt als Instrument der innerbetrieblichen Selbstkontrolle die umfassende datenschutzrechtliche Kontrollfunktion über die verantwortliche Stelle vor.

Grundsatzentscheidung des Bundesarbeitsgerichts

(Beschluss v. 11.11.1997 - Az. 1 ABR 21/97): (-)

Entscheidung aber zu altem BDSG (vor Umsetzung der EU Datenschutz-RL 95/46/EG)

Politische Diskussion: Kontrollrecht in Entwurf BeschDSG vorgesehen!

[P] Unabhängigkeit des DSB vom Arbeitgeber?

-> § 4f BDSG

- Bestellung: **(-)** einseitige Auswahl + Bestellung durch Arbeitgeber
- Tätigkeit: **(+)** weisungsfreie Tätigkeit
- Nach Beendigung: **(+)** Kündigungsschutz

Pflicht zur Benennung von Arbeitnehmern gegenüber BR: "BEM"

-> BAG, Beschluß v. 07.02.2012 - 1 ABR 46/10

Leitsatz

Der Betriebsrat kann verlangen, dass ihm der Arbeitgeber die Arbeitnehmer benennt, welche nach § 84 Abs. 2 SGB IX die Voraussetzungen für die Durchführung des betrieblichen Eingliederungs-managements erfüllen.

Orientierungssätze

1. Die Benennung der Arbeitnehmer ist zur Durchführung der sich aus § 80 Abs 1 Nr 1 BetrVG, § 84 Abs 2 S 7 SGB IX ergebenden Überwachungsaufgabe erforderlich.

2. Der Arbeitgeber muss dem Betriebsrat die Namen der Arbeitnehmer mit Arbeitsunfähigkeitszeiten von mehr als sechs Wochen im Jahreszeitraum auch dann mitteilen, wenn diese der Weitergabe nicht zugestimmt haben. Die Überwachungsaufgabe des Betriebsrats nach § 80 Abs 1 Nr 1 BetrVG ist nicht von einer vorherigen Einwilligung der von der Vorschrift begünstigten Arbeitnehmer abhängig. Eine solche Einschränkung folgt auch nicht aus § 84 Abs 2 SGB IX.

3. Der Übermittlung der Namen stehen auch keine datenschutzrechtlichen Gründe entgegen. Das Erheben von Daten über die krankheitsbedingten Fehlzeiten durch den Arbeitgeber und ihre Übermittlung an den Betriebsrat ist auch bei fehlender Zustimmung der betroffenen Arbeitnehmer nach § 28 Abs 6 Nr 3 BDSG zulässig.

Kein MBR des BR bei Installation einer Kamera-Attrappe durch den AG

-> LAG Rostock *(Beschluss vom 12.11.2014 - 3 TaBV 5/14)*

Leitsatz

Das Anbringen der Attrappe einer Videokamera im Außenbereich eines Klinikgebäudes erfüllt offensichtlich keinen Mitbestimmungstatbestand i.S.d. § 87 BetrVG.

Aus den Gründen:

Ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG scheidet bereits auf den ersten Blick ersichtlich aus, da eine Kameraattrappe jedenfalls objektiv nicht geeignet ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

Sinn und Zweck von § 87 Abs. 1 Nr. 6 BetrVG ist der Schutz des allgemeinen Persönlichkeitsrecht des Arbeitnehmers vor Eingriffen durch anonyme technische Kontrolleinrichtungen. Derartige Eingriffe sind von einer Attrappe ersichtlich nicht zu erwarten.

Auch ein Mitbestimmungsrecht nach § 87 Abs. 1 Satz 1 BetrVG ist nicht ersichtlich. Die Anbringung der Attrappe einer Videokamera im Außenbereich entfaltet schon auf den ersten Blick keine Auswirkungen auf das innerbetriebliche Zusammenleben der Arbeitnehmer.
Die Arbeitnehmer können den betroffenen Eingang nach wie vor betreten und verlassen, ohne neuen zusätzlichen Regelungen des Zusammenlebens unterworfen zu sein, die vom Betriebsrat mitgestaltet werden könnten.

Wirksamkeit einer Betriebsvereinbarung: „Taschenkontrolle"

-> BAG, Urteil v. 15.04.2014 - 1 ABR 2/13 (B)

4. Durchführung der Torkontrollen: Zum Schutze des persönlichen und betrieblichen Eigentums werden aus den Ausgangsdrehkreuzen durch dazu bestimmten Personen Kontrollen durchgeführt. Alle Betriebsangehörigen haben auf Verlangen über Betriebsprodukte in ihrem Besitz einen Nachweis vorzuzeigen (Kassenbon Personalverkauf). Durch die beim Verlassen des Werkes notwendige Öffnung der Drehkreuze mittels des Werksausweises wird eine Auswahl der zu kontrollierenden Personen über einen Zufallsgenerator getroffen. Der Kontrollzyklus wird dem Betriebsrat mitgeteilt. Bei Verlassen des Werksgeländes über die Pforte, kann ebenfalls jederzeit eine Kontrolle durchgeführt werden.
Die Kontrolle findet im Pförtnerraum an einer nicht einsehbaren Stelle statt. Die Kontrolle bezieht sich auf die Durchsicht mitgeführter Behältnisse, Jacken- und Manteltaschen. In begründeten Verdachtsfällen wird der Mitarbeiter aufgefordert sämtliche Kleidertaschen (Hosen und Kleider) zu leeren. Weigert sich der Mitarbeiter dem nachzukommen, kann die Kontrolle auf Veranlassung der Firma, durch die zuständige Polizei durchgeführt werden. Über jede durchgeführte Kontrolle wird ein Protokoll angefertigt. Dieses Protokoll ist von demjenigen zu unterzeichnen, der die Kontrolle durchgeführt hat und von dem/der betroffenen Mitarbeiter/in gegenzuzeichnen. Es dient als Nachweis der Durchführung sowie hinsichtlich etwaig beschlagnahmter Gegenstände.

Aus den Gründen:

Die Taschenkontrollen sind geeignet, das Eigentum der Arbeitgeberinnen zu schützen. Da hierdurch Diebstähle aufgedeckt werden können und durch die Auswahl der zu kontrollierenden Arbeitnehmer über einen Zufallsgenerator die Beschäftigten jederzeit damit rechnen müssen, kontrolliert zu werden, entfaltet dieses Überwachungssystem repressive wie präventive Wirkung.

Die Taschenkontrollen sind erforderlich. Andere, gleich wirksame und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkende Mittel stehen den Betriebsparteien zum Schutz des Eigentums der Arbeitgeberinnen vor Diebstählen nicht zur Verfügung. Eine Kameraüberwachung bei Verlassen des Betriebsgeländes wäre nicht gleich wirksam, da mitgeführte Gegenstände in Taschen oder Behältnissen nicht erkannt werden könnten. Eine Videoüberwachung in den Arbeitsbereichen würde das allgemeine Persönlichkeitsrecht der Arbeitnehmer stärker beeinträchtigen, da diese einer dauerhaften Beobachtung ausgesetzt wären.

Die Kontrollmaßnahmen tragen dem Gebot der Verhältnismäßigkeit im engeren Sinn Rechnung. Die Arbeitgeberinnen haben unbestritten vorgetragen, im Rahmen von Inventuren sei ein Schaden in einer Größenordnung von ca. 250.000,00 Euro *[entstanden]*. Im Hinblick darauf haben die Betriebsparteien zum Schutz des Eigentumsrechts der Arbeitgeberinnen aus Art. 14 Abs. 1 GG Regelungen getroffen, die nur geringfügige Beeinträchtigungen des durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechts bewirken.

Rechtsprechungs-“Basics“ zur IKT-Nutzung des Betriebsrats:

LAG Hamburg

- Recht des BR zur Nutzung personenbezogener Mitarbeiterdaten
  Urteil v. 26.11.2009 – Az. 7 TaBV 2/09

LAG Berlin-Brandenburg

- Konfiguration des BR-PC, Gruppenaccount für alle BR-Mitglieder
  Beschluss v. 04.03.2011 – Az. 10 TaBV 1984/10

BAG

- Elektronisches Leserecht für Dateien / E-Mail-Korrespondenz des BR
  Beschluss v. 12.08.2009 – 7 ABR 15/08

ArbG Bielefeld

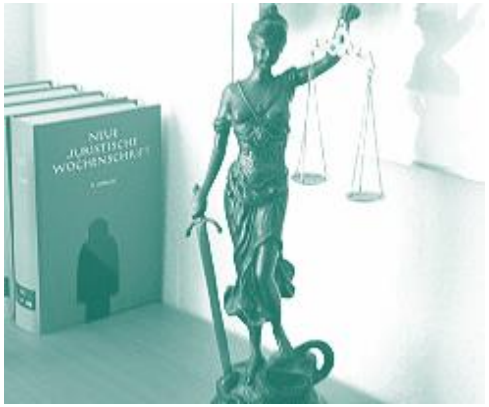
- Datenmißbrauch durch den BR-Vorsitzenden
  Beschluß v. 26.01.2011 – Az. 6 BV 46/2010

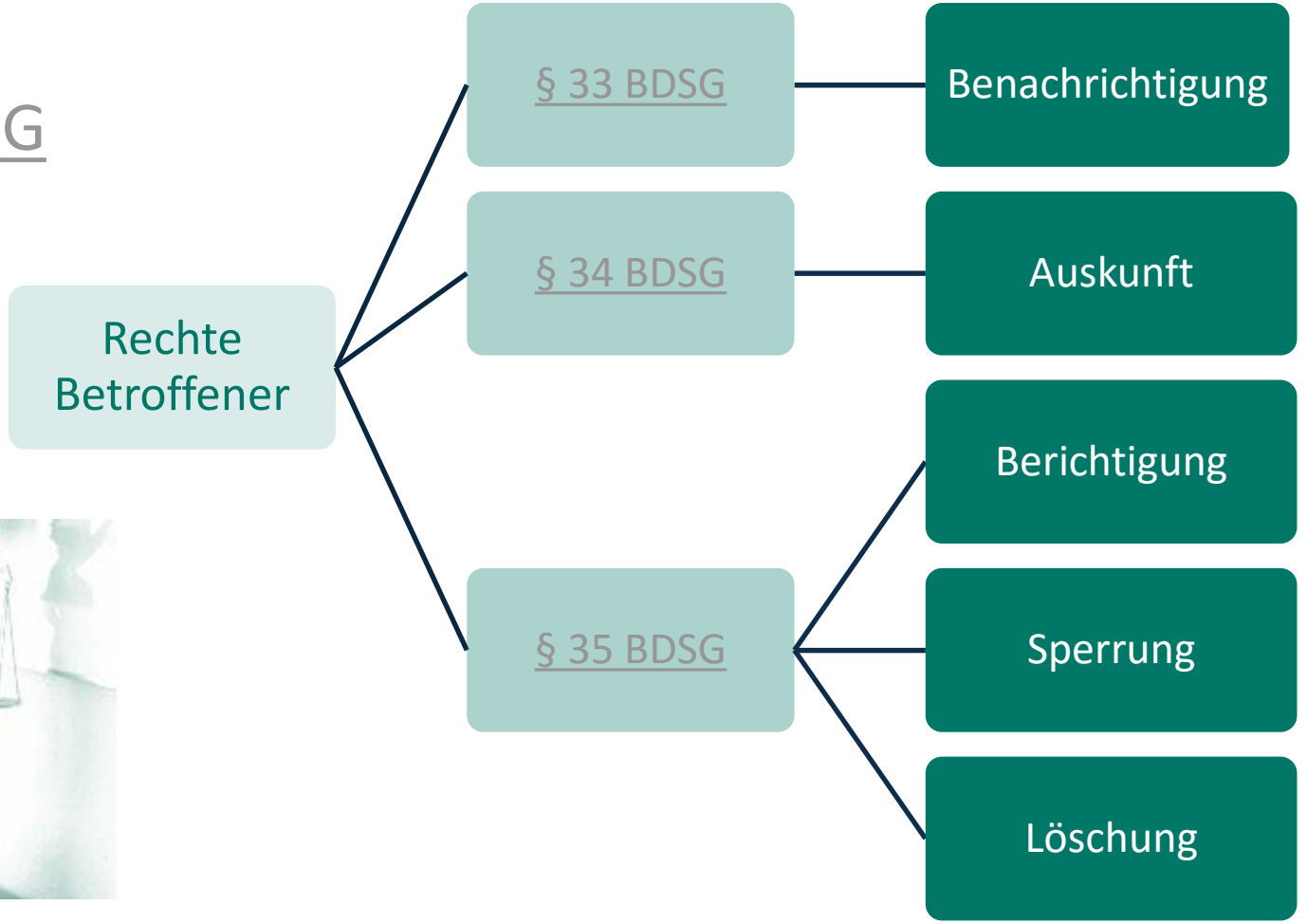
Standort

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

Übersicht

§§ 33-35 BDSG





Unterrichtungspflichten des Arbeitgebers

Informationspflichten zugunsten der betroffenen Arbeitnehmer

- Vor Datenerhebung beim Betroffenen, § 4 Abs. 3 BDSG
- Bei erstmaliger Speicherung, § 33 BDSG
- Vor Einwilligung in die Datenverarbeitung, § 4a BDSG
- Im Rahmen der Video-Überwachung, § 6b BDSG
- Im Rahmen der Nutzung mobiler Speichermedien, § 6c BDSG
- Bei unrechtmäßiger Kenntnis-erlangung, § 42a BDSG
- u.U. Informationspflicht aus allg. zivilrechtlichen Grundsätzen

Meldepflichten zugunsten des Datenschutz-Beauftragten

- Vor Inbetriebnahme automatisierter Verfahren, § 4 d BDSG
- Bei Vorhaben automatisierter Verarbeitung, § 4 g BDSG
- Bei Einrichtung automatisierter Abrufverfahren, § 10 BDSG

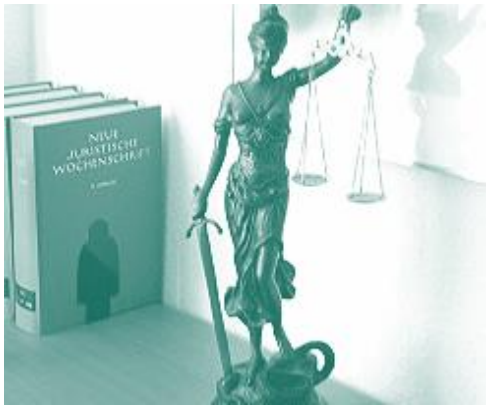
Auskunftsrechte der betroffenen Arbeitnehmer

- Betroffener über die zu seiner Person gespeicherten Daten, § 34 BDSG
- Sonstige Auskunftsrechte außerhalb des BDSG, z.B. § 83 BetrVG, Betriebsvereinbarung, Tarifvertrag

Weitere Pflichten möglich durch im Unternehmen durch TV oder BV geltende Regelungen

Benachrichtigung des Betroffenen

§ 33 BDSG



Voraussetzungen

- Erstmalige Speicherung
- personenbezogener Daten
- für eigene Zwecke
- ohne Kenntnis des Betroffenen

Inhalt des Auskunftsanspruchs

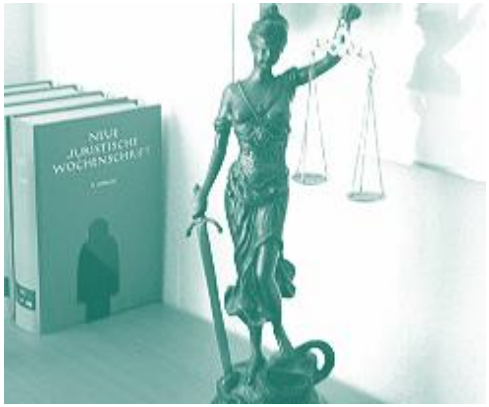
- Die Speicherung als solche
- Art der Daten
- Zweck der Erhebung
- Identität der verantwortlichen Stelle
- Kategorien von Empfängern

Entbehrlichkeit der Benachrichtigung, § 33 Abs. 2 BDSG

- Vorhandene Kenntnis des Betr. von der Speicherung, Nr. 1
- Unverhältnismäßiger Aufwand, Nr. 2
- Schutzwürdiges Geheimhaltungsinteresse, Nr. 3
- Wissenschaftsprivileg, Nr. 5
- Gefährdung d. öff. Sicherheit, Nr. 6
- Daten aus allg. zugängl. Quellen, Nr. 7a
- Gefährdung eig. Geschäftszwecke, Nr. 7b
- Vom Betroffenen veröffentlichte Daten, Nr. 8

Auskunftsrechte des Betroffenen

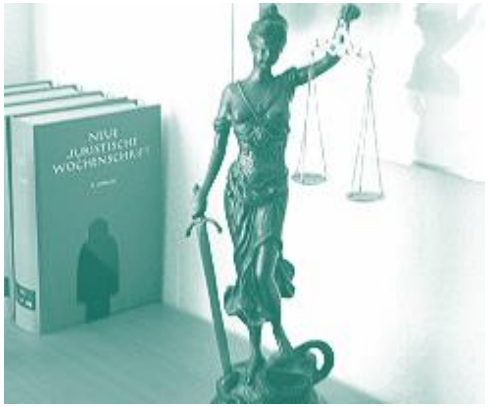
§ 34 BDSG



Voraussetzungen	• Auskunftsverlangen des Betroffenen
Inhalt des Auskunftsanspruchs	• Die zur Person gespeicherten Daten • Herkunft der Daten • Bezeichnung der Datei, in der die Daten gespeichert sind • Zweck der Speicherung • Empfänger und Kategorien von Empfängern
Einschränkung des Auskunftsanspruchs, § 34 Abs. 7 i.V.m. § 33 Abs. 2 S. 1 Nrn. 2,3, 5-7	• Unverhältnismäßiger Aufwand, Nr. 2 • Schutzwürdiges Geheimhaltungsinteresse, Nr. 3 • Wissenschaftsprivileg, Nr. 5 • Gefährdung d. öff. Sicherheit, Nr. 6 • Daten aus allg. zugängl. Quellen, Nr. 7a • Gefährdung eig. Geschäftszwecke, Nr. 7b

Benachrichtigungspflicht bei „Datenpannen“

§ 42a BDSG



Relevant nicht nur für echte „Pannen“ sondern insbes. auch bei regelmäßigen Datentransfers innerhalb Konzernstruktur!

Voraussetzungen

- **Unrechtmäßige Übermittlung oder unrechtmäßige Kenntniserlangung durch Dritte auf sonstige Weise**
- **besonders sensibler Daten:**
  - bApbD, § 3 Abs. 9 BDSG (Nr. 1)
  - pbD, die Berufsgeheimnis unterliegen (Nr. 2)
  - pbD, die sich auf strafbare Handlungen / Owi oder entspr. Verdacht beziehen (Nr. 3)
  - pbD zu Bank- oder Kreditkartenkonten (Nr. 4)
- **Adressat: ö/nö verantwortl. Stellen i.S.d. § 27 Abs. 1 S. 1 Nr. 2 BDSG [P] ADV? Wohl (-)**
- **Gefahr einer schwerwiegenden Beeinträchtigung f.d. Rechte oder schutzwürdigen Interessen d. Betroffenen**

Folge der Kenntniserlangung

- **Ergreifung angemessener Maßnahmen zur Datensicherung**
- **Unverzügliche Benachrichtigung des Betroffenen über**
  - Art der Daten
  - Darlegung der unrechtmäßigen Kenntniserlangung
  - Empfehlungen für Maßnahmen zur Minderung von Folgen
- **Unverzügliche Benachrichtigung der Aufsichtsbehörde über mögliche Folgen und Angabe der ergriffenen Maßnahmen**

Standort

VDAA - Verband deutscher ArbeitsrechtsAnwälte e.V.

Übersicht

Rechtsfolgen einer rechtswidrigen Datenverarbeitung

Zivilrecht

Betroffener AN gegen AG

Zurückbehaltungs-Recht
§ 273 I BGB
[P]: Erheblichkeit

Schadensersatz
§§ 7,8 BDSG,
§ 280 I S. 1 BGB,
§ 823 I + II BGB,
§ 824 BGB,
§ 826 BGB,
§ 839 BGB iVm Art 34 GG

Unterlassung, Beseitigung, Gegen-darstellung,
§ 823 I iVm § 1004 BGB analog bzw. APR,
Löschung,
§ 35 II BDSG

Herausgabe, Gewinn-abschöpfung, § 812 I 1 Alt. 2 BGB + § 823 I iVm APR

Betroffener AN gegen Handelnden

Schadensersatz,
§§ 823 ff. BGB;
Zurechnung: §§ 31, 278, 831 BGB, § 11 I S. 2 BDSG

StGB

§ 201
§ 202
§ 202a
§ 202b
§ 203
§ 206
§ 303a
§ 303b
§ 17 UWG

OWi

§ 43 BDSG

§ 149 TKG

Beachte:
§ 44 Abs. 1 i.Vm. § 43 Abs. 2 BDSG = Straftat!

Bußgelder

„You think compliance is expensive? Try non-compliance!"

§ 43 BDSG

Abs. 1 = bis EUR 50.000

- Verstoß gegen die Meldepflicht
- Fehlende, nicht rechtzeitige oder nicht ordnungsgemäße (z.B. fehlende Fachkunde) Bestellung eines Datenschutzbeauftragten
- Verstoß gegen eine Anordnung der Aufsichtsbehörde
- Fehlende Protokollierung bei automatisierten Abrufverfahren
- Pflichtverletzung bei der Auftragsdatenverarbeitung
- Wenn die Benachrichtigung über die Datenerhebung gegenüber dem Betroffene nicht, nicht richtig oder nicht rechtzeitig erfolgt
- Fehlende Widerrufsbelehrung bei einer werblichen Ansprache
- Unzulässige Übermittlung und Nutzung von Daten entgegen ihrem Zweck
- Verstoß gegen die Dokumentationspflichten bei der Datenübermittlung zu Geschäftszwecken
- Wenn eine Auskunft gegenüber einem Betroffenem nicht, unvollständig, verspätet oder falsch erfolgt

Abs. 2 = bis EUR 300.000

- Unbefugte Erhebung und Verarbeitung von personenbezogene Daten, die nicht allgemein zugänglich sind
- Unbefugte Bereithaltung von personenbezogenen Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahren
- Unbefugter Abruf von personenbezogenen Daten, die nicht allgemein zugänglich sind
- Erschleichen von Übermittlungen von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben
- Nutzen von Daten entgegen ihrer Zweckbindung
- Missachtung des Kopplungsverbotes (d.h. wenn der Abschluss eines Vertrages von der Einwilligung zur Datennutzung abhängig ist, obwohl diese nicht zwingend erforderlich ist)
- Nutzen von personenbezogenen Daten zum Zwecke der Werbung, Markt- und Meinungsforschung, obwohl ein Widerspruch vorliegt.
- De-Anonymisieren von anonymisierten Daten
- Wenn eine nicht-öffentliche Stelle feststellt, dass sie unrechtmäßig besondere Arten von Daten (z.B. Gesundheitsdaten, Berufsgeheimnisse etc.) übermittelt hat und dies nicht der Aufsichtsbehörde meldet

Bußgelder werden tatsächlich auch verhängt…

„You think compliance is expensive? Try non-compliance!"

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

Ansbach, den 20. August 2015

Pressemitteilung

„Auftragsdatenverarbeitung ohne richtigen Vertrag kann teuer werden"

Wer andere für sich mit personenbezogenen Daten arbeiten lässt, muss darüber Kraft Gesetzes einen ziemlich detaillierten Vertrag schließen. Wird so ein Vertrag nicht oder unzureichend abgeschlossen, droht ein Bußgeld. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat kürzlich im Fall einer unzureichenden Auftragserteilung eine Geldbuße in fünfstelliger Höhe festgesetzt.

Wer einen externen Dienstleister als so genannten Auftragsdatenverarbeiter mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt, muss mit diesem einen schriftlichen Vertrag abschließen. Das Gesetz schreibt eine Reihe von Einzelheiten vor, die zum Schutz der personenbezogenen Daten darin ausdrücklich festgelegt werden müssen. Von besonderer Bedeutung sind dabei die technischen und organisatorischen Maßnahmen (Datensicherheitsmaßnahmen), die der Auftragsdatenverarbeiter zum Schutz der Daten treffen muss. Diese Maßnahmen müssen im schriftlichen Auftrag konkret und spezifisch festgelegt werden. Fehlen konkrete Festlegungen hierzu, stellt dies eine Ordnungswidrigkeit dar, die mit Geldbuße von bis zu 50.000,- € geahndet werden kann.

Das BayLDA hat kürzlich gegen ein Unternehmen eine Geldbuße in fünfstelliger Höhe festgesetzt. Das Unternehmen hatte in seinen schriftlichen Aufträgen mit mehreren Auftragsdatenverarbeitern keine konkreten technisch-organisatorischen Maßnahmen zum Schutz der Daten festgelegt. Stattdessen enthielten die Aufträge nur einige wenige pauschale Aussagen und Wiederholungen des Gesetzestextes. Dies reicht keinesfalls aus. Denn die datenschutzrechtliche Verantwortung trägt auch im Falle der Einschaltung von Auftragsdatenverarbeitern nach wie vor der Auftraggeber. Dieser muss daher beurteilen können, ob der Auftragsdatenverarbeiter in der Lage ist, für die Sicherheit der Daten zu sorgen. Auch muss der Auftraggeber die Einhaltung der technisch-organisatorischen Maßnahmen bei seinem Auftragnehmer kontrollieren.

Hierfür ist es unerlässlich, dass die beim Auftragsdatenverarbeiter zum Schutz der Daten zu treffenden technisch-organisatorischen Maßnahmen in dem abzuschließenden schriftlichen Auftrag spezifisch festgelegt werden. Nur so kann der Auftraggeber beurteilen, ob die personenbezogenen Daten bei seinem Auftragnehmer z. B. gegen Auslesen oder Kopieren durch Unbefugte, gegen Verfälschung oder sonstige unberechtigte Abänderung oder gegen zufällige Zerstörung geschützt sind.

…nicht nur in Bayern!

„You think compliance is expensive? Try non-compliance!"

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

Ansbach, den 28. Juni 2013

Pressemitteilung

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat gegen eine Mitarbeiterin eines Unternehmens ein Bußgeld verhängt, weil sie mit einem offenen E-Mail-Verteiler personenbezogene E-Mail-Adressen einem großen Empfängerkreis übermittelt hat.

Eine Mitarbeiterin eines Handelsunternehmens hat an Kunden eine E-Mail verschickt, die ausgedruckt zehn Seiten umfasst, wobei neuneinhalb Seiten die E-Mail-Adressen ausmachen und eine halbe Seite die Information beinhaltete, dass man sich zeitnah um die Anliegen der Kunden kümmern werde.

E-Mail-Adressen, die sich in erheblichem Umfang aus Vornamen und Nachnamen zusammensetzen, sind als personenbezogene Daten im Sinne des Datenschutzrechts anzusehen. Diese personenbezogenen Daten dürfen an Dritte nur dann übermittelt werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Grundlage gegeben ist. Beide Voraussetzungen lagen hier nicht vor. Die Verwendung dieses offenen E-Mail-Verteilers (Eintragung der EMail- Adressen in das "AN-Feld") stellte damit einen Datenschutzverstoß dar, der mit einem Bußgeld geahndet werden kann. Im Hinblick auf die erhebliche Anzahl der E-Mail-Adressen hat es das BayLDA in diesem Fall nicht mehr bei einer (folgenlosen) Feststellung der datenschutzrechtlichen Unzulässigkeit belassen, sondern ein Bußgeld verhängt. Der entsprechende Bußgeldbescheid ist nach Ablauf der Einspruchsfrist unanfechtbar geworden.

Das BayLDA hat bereits unabhängig von diesem Fall mehrfach darauf hingewiesen, dass die Verwendung eines offenen E-Mail-Verteilers datenschutzrechtlich unzulässig ist, wenn die Inhaber der E-Mail-Adressen dazu nicht ihre Einwilligung erklärt haben. Es ist auch dem BayLDA bekannt, dass ein derartiger Verstoß sehr schnell und fahrlässig geschehen kann, wenn man die E-Mail-Adressen in das „AN-Feld" oder das „CC-Feld" einträgt und nicht in das „BCC-Feld". Bei Eintragung der E-Mail-Adressen in das „AN-Feld" oder das „CC-Feld" sehen sowohl die unmittelbaren Empfänger („AN-Feld") als auch die Empfänger der Kopien („CCFeld") dieser Mail, an wen die Mail sonst noch geschickt wurde. Nur bei Eintragung der EMail- Adressen in das „BCC-Feld" (englisch:

***B**lind **C**arbon **C**opy*, dt. sinngemäß *Blindkopie*) wird die Übertragung der E-Mail-Adressen an die Empfänger unterdrückt, so dass keiner erkennen kann, an wen diese Mail sonst noch geschickt wurde.

Da in manchen Unternehmen dieser Fragestellung offensichtlich nicht die entsprechende Bedeutung beigemessen wird, d.h. von Seiten der Unternehmensleitung die Mitarbeiter entweder nicht entsprechend angewiesen oder überwacht werden, wird das BayLDA in einem vergleichbaren Fall in Kürze einen Bußgeldbescheid nicht gegen den konkreten Mitarbeiter, der die Mail mit offenem E-Mail-Verteiler versandt hat, erlassen, sondern gegen die Unternehmensleitung.

Jan A. Strunk

- Kontakt
  strunk@hsv-fl.de
- XING
  www.xing.com/profile/JanA_Strunk
- LinkedIn
  http://de.linkedin.com/in/foerdeanwalt

HOECK SCHLÜTER VAAGT
Rechtsanwälte Partnerschaft mbB
Lise-Meitner-Straße 15 - 24941 Flensburg
fon + 49 461 / 903 60 0 | fax + 49 461 / 903 60 80
www.hsv-fl.de

LEGALIT.de
::: IKT | Arbeit | Medien | Recht :::