

Datenschutz – Ein Grundrecht für alle setzt sich durch (?)

ZUKUNFTSWERKSTATT

13. und 14. Oktober 2010

Pforzheim-Hohenwart

Ihr Referent



Thorsten Jordan

- Gesellschafter-Geschäftsführer der jordan Wirtschaftsberatung GmbH,
- Unternehmensberater u. Wirtschaftscoach,
- Sachverständiger für Unternehmensplanung im BDSF e.V.,
- Lehrbeauftragter für Projektmanagement,
- Externer Datenschutzbeauftragter (IHK)
- Dozent und Mitglied von **Team** Datenschutz

Inhalte

In diesem Workshop erfahren Sie...

- Was Datenschutz ist und was personenbezogene Daten sind
- Folgen von Datenschutzverletzungen
- Warum Sie Ihr Arbeitgeber auf das Datengeheimnis verpflichtet
- Relevanz von Arbeitnehmerdatenschutz
- Grundprinzipien des Datenschutzes
- 10 konkrete Handlungsempfehlungen für Ihre tägliche Arbeit

Datenschutz – das tägliche Chaos

- April 2009: Drogeriekette Müller horcht Mitarbeiter aus
- November 2009: Nach Datendiebstahl tauschen deutsche Banken hunderttausende VISA und Mastercards aus
- Januar 2010: Regierung startet Projekt „ELENA“ und sammelt mit dem elektronischen Entgeltnachweis Daten über Arbeitnehmer
- März 2010: LKW eines Telekommunikations- und Kabel-TV-Anbieters verliert hunderte Zettel mit tausenden persönlichen Daten von der Ladefläche
- Mai 2010: Panne bei Vodafone: MobileMails fremder Kunden einsehbar
- Mai 2010: Neuer Datenskandal bei SchülerVZ: 1,6 Mio. Datensätze abgefischt
- Juli 2010: Bußgeldverfahren gegen Facebook eingeleitet

Datenschutz aktuell

„Projekt Datenschutz“
Datenschutzvorfälle in Unternehmen, Organisationen und Behörden und Datenschutz-Aktivitäten der Politik

Suche nach: Suchen

Home
Das Projekt
News
Blog „Datenschutz“
Links
Twitter
Kontakt/Impressum

Datum	Ort	Datenherkunft	Organisation	Betroffene	Anz. Betroffene	Kurzbeschreibung	
01.09.2010	Bonn	Artegit AG	Unternehmen	Schlecker-Newsletter-Kunden	Unzählige	Datenleck beim Dienstleister von Schlecker	Details...
27.08.2010	Ehingen	Schlecker	Unternehmen	Schlecker-Kunden	7,1 Millionen	Schlecker-Kundendatenbank offen zugänglich im Internet	Details...
23.08.2010	Oberursel	Alte Leipziger	Unternehmen	Versicherungs-Kunden	3.600	Tausende Datensätze der Alte-Leipziger-Versicherung standen ungeschützt zum Download bereit	Details...
19.08.2010	Hamburg	Unbekannt	Unternehmen	Kreditkartenbesitzer	800	Computer-Bild: 800 Kreditkarten-Datensätze per Mail erhalten	Details...
05.08.2010	Regensburg	GEZ	Behörde	Regensburger	Hunderte	GEZ-Fahnder verliert Karteikarten auf der Straße	Details...
04.08.2010	Südharz	Gemeindeverwaltung	Öffentliche Verwaltung	Personalrätin	1	Datenkandal im Verwaltungsamt: Bürgermeister spioniert neue Personalrätin aus	Details...
03.08.2010	Aalen	Arztpraxis	Unternehmen	Patienten	Mehrere	Krankenakten landen im Müll	Details...
27.07.2010	Aachen	Mädchen	Einzelperson	Mädchen	Hunderte	Spanner spähte hunderte Mädchen via Webcam aus	Details...
23.07.2010	Bönen	Creditreform	Unternehmen	Mitarbeiter	Tausende	KIK spähte Finanzdaten von Mitarbeitern aus	Details...
23.07.2010	Waldeck-Frankenberg	Kreisverwaltung	Behörde	Mitarbeiter	Hunderte	Kreisverwaltung Waldeck-Frankenberg spionierte Computer von Mitarbeitern aus	Details...
06.07.2010	Bremen	SV Werder Bremen	Verein	Mitglieder und Kunden	34.700	Datenpanne beim SV Werder Bremen legt Kontodaten aller Mitglieder offen	Details...
21.06.2010	München	Arztpraxis	Unternehmen	Patienten	Hundert	Münchener Arzt entsorgt Patientenakten in der Mülltonne	Details...
21.06.2010	Garching	Werner-Heisenberg-Gymnasium	Bildungseinrichtung	Schüler	Mehrere	Gymnasium veröffentlicht Liste mit chronischen Krankheiten von Schülern	Details...
21.06.2010	Sachsen-Anhalt	Landtag	Behörde	Abgeordnete	Hunderte	Datenpanne im Magdeburger Landtag	Details...
16.06.2010	München	Stadtverwaltung	Öffentliche Verwaltung	Briefwähler	15.000	Datenleck beim Wahlamt München löst munteren Handel mit hochsensiblen Daten aus	Details...
14.06.2010	Dessau	Polizeidirektion	Behörde	Beamte	400	Polizei in Sachsen-Anhalt spähte eigene Beamte aus	Details...
14.05.2010	München	Bayerisches Landesamt für Steuern	Behörde	Privatpersonen	Hunderte	Festplatten mit brisanten Steuerdaten auf Flohmarkt aufgetaucht [Update]	Details...
14.05.2010	Göttingen	Rote Hilfe e.V.	Verein	Mitglieder	Tausende	Rote Hilfe e.V.: Festplatte mit Mitgliederdaten gestohlen	Details...
12.05.2010	Düsseldorf	Vodafone	Unternehmen	Vodafone-Kunden	Einzelne	Panne bei Vodafone: Mobilnummern fremder Kunden einsehbar	Details...
04.05.2010	Berlin	SchülerVZ	Unternehmen	SchülerVZ-Mitglieder	1,6 Millionen	Neuer Datenkandal bei SchülerVZ: 1,6 Millionen Datensätze abgefischt	Details...

1 2 3 4 5 6 7 8 nächste Seite > letzte Seite >>

[Weiteren Datenvorfall melden](#)

→ www.projekt-datenschutz.de

Datenschutz verzeiht keine Fehler

- April 2008
 - bei Lidl wurden Mitarbeiter und Kunden per Kamera überwacht
 - Marktanteil sinkt von 12,8% auf 9,4%, erst im September wieder normal
- September 2008
 - Bußgeldbescheid über 1,44 Mio. € wird sofort bezahlt
 - (300 Einzelfälle)
- Februar 2009
 - Krankendaten von Lidl-Mitarbeitern werden im Müll gefunden
- Februar 2009
 - GF bei Lidl wird gefeuert
- 2009: Lidl startet Imagekampagne
- Gesamtschaden: ca. 100 Mio. Euro

Denn sie wissen, was wir tun

Amazon, der Internet-Versandhandel, kennt unsere Lesegewohnheiten und unseren Musikgeschmack besser als wir selbst

Payback: unsere Einkaufsgewohnheiten werden genauestens analysiert

Handy: wo wir uns bewegen, kann minutiös nachvollzogen werden

Internet: wir hinterlassen vielfältige elektronische Spuren, die nur sehr schwer wieder zu löschen sind

Kundenkarten: je nach Art kann genau nachvollzogen werden, dass wir z.B. gerade eine Diät machen, weil wir entsprechende Lebensmittel einkaufen, dass wir eine Allergie haben, weil wir bestimmte Lebensmittel meiden. Die Technik der Auswertung im Handel ist hier sehr weit

Kreditkarten: wir bezahlen im Restaurant, unsere Reisen, beim Tanken, beim Einkaufen, im Internet und bei vielen weiteren Gelegenheiten mit Kreditkarten. Die Kreditkartenunternehmen kennen uns sehr genau.

Autobahn-Fahrt: Etwa jede 2. oder 3. Mautbrücke macht Fotos von uns und unserem Nummernschild. So werden ca. alle 10 km 2 hochauflösende Fotos gemacht, jedes Mal etwa 1-2 MB Daten.

Dieses sind **nur einige Beispiele**. Sie erklären jedoch, warum immer mehr Menschen immer sensibler beim Datenschutz reagieren.

Datenschutz – ein Grundrecht

Was schätzen Sie, wie lange schon gibt es den Datenschutz?

Seit weit mehr als 2.000 Jahren. Der griechische Arzt Hippokrates war der erste uns Bekannte, der in seiner Selbstverpflichtung („Eid des Hippokrates“) für Ärzte Regeln einfließen ließ, die wir heute beim Datenschutz kennen.

1970 – das weltweit erste Datenschutzgesetz entsteht in Hessen

1983 – das Bundesverfassungsgericht postuliert das neue Grundrecht auf informationelle Selbstbestimmung. Jeder Mensch soll im Rahmen des Rechts auf freie Entfaltung der Persönlichkeit selbst bestimmen dürfen, wer seine Daten erhält.

1995 – die EU-Richtlinie zum Datenschutz verpflichtet alle Mitgliedsstaaten, ein nationales Datenschutzgesetz nach einheitlichen EU-Standards zu erlassen.

2000, 2003, 2006 und 2009/2010 – das Bundesdatenschutzgesetz wird jeweils aktualisiert. Als nächstes wird der Arbeitnehmerdatenschutz in das Gesetz eingeflochten.

Einführungsbeispiel

- Stellen Sie sich einen Patienten in einer Arztpraxis vor.
- Er leidet unter multipler Sklerose, eine derzeit unheilbare Krankheit. Arbeiten kann der Betreffende sehr gut. Bis auf seltene Schübe gibt es kaum Beeinträchtigungen.
- Gerade bewirbt er sich für eine neue Stelle.
- Die Patientenkartei liegt offen auf dem Tresen. Ein Mitarbeiter des Wunscharbeitgebers sieht zufällig die Diagnose.
- Der Betreffende bekommt den Job nicht. Er erfährt zufällig, warum er die Stelle nicht bekommen haben.
- Welche Folgen hat diese Aktion?

Warum Datenschutz?

7 gute Gründe für den Datenschutz

- Kunden/, Mitarbeiter und Lieferanten erwarten selbstverständlich Einhalten des Datenschutzes
- Immer häufiger wird die Erteilung eines Auftrags an den Nachweis eines funktionierenden Datenschutz gebunden
- Auditoren verlangen den Nachweis, dass Datenschutz und (IT-)Sicherheit umgesetzt werden
- Bei Kapitalgesellschaften: persönliche Haftung des Geschäftsführers bei (IT-)Sicherheit und Datenschutz
- Datenschutz kann Image fördernd wirken
- Datenschutz als Voraussetzung für Prozessoptimierung bei den Verwaltungsgeschäftsprozessen
- Last, but not least: Datenschutz ist europaweit gesetzlich gefordert

Warum/Wann Datenschutzbeauftragte/r?

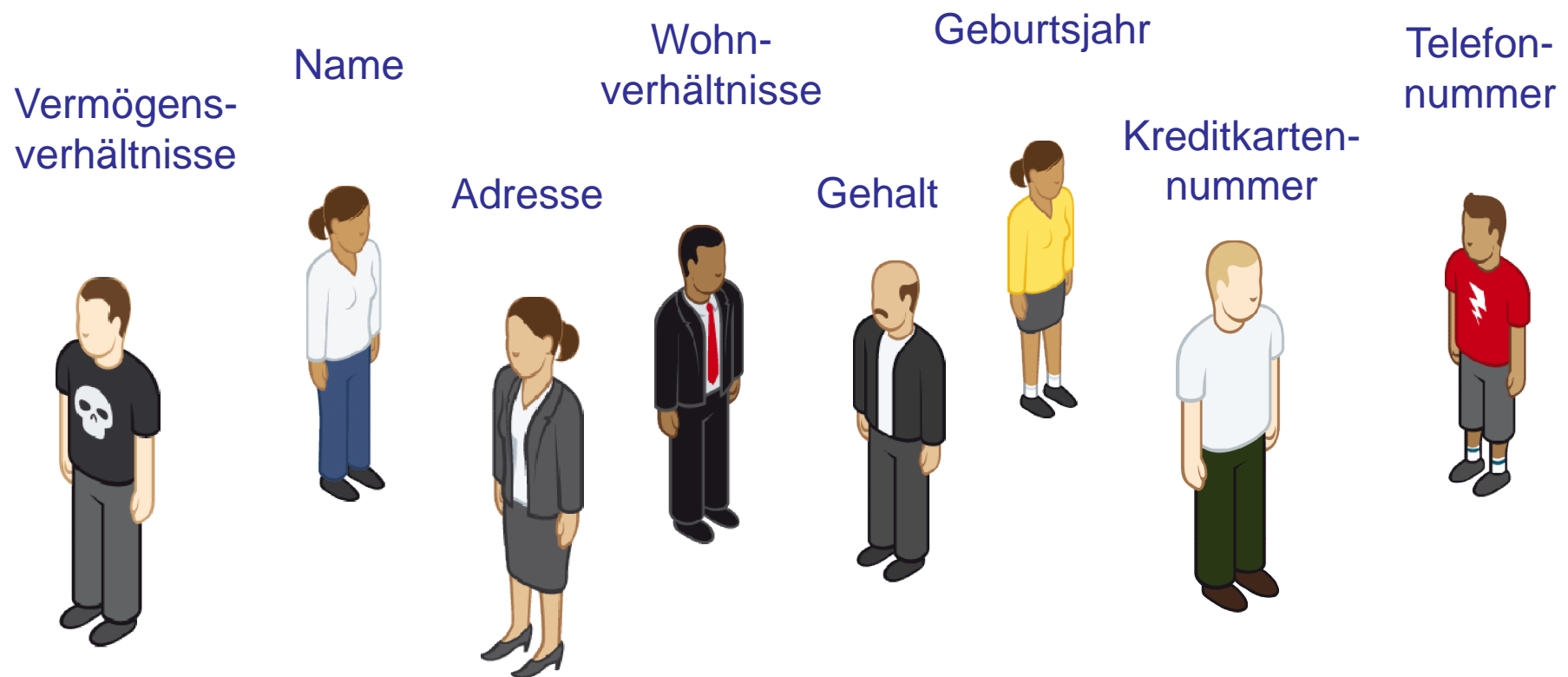
- Alle Unternehmen müssen Datenschutzkonzept umsetzen
- Bei mehr als neun Personen, die ständig, automatisiert, personenbezogene Daten verarbeiten, oder bei erforderlicher Vorabkontrolle muss ein Datenschutzbeauftragter bestellt werden
- Weniger als 20 % der Unternehmen erfüllen diese Anforderungen
- Bei Verstößen: Bußgelder bis 300.000 € drohen, bei Vorsatz und Wille zur Bereicherung auch Freiheitsstrafe bis zu 2 Jahren
- Derzeit kaum Kontrollen, Tendenz zunehmend

Intention Datenschutz

- Den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird
- Datenschutzrecht gilt in der EU einheitlich
- Legitimation: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur in bestimmten Ausnahmefällen erlaubt (Verbot mit Erlaubnisvorbehalt):
 - wenn das Datenschutzgesetz dies ausdrücklich erlaubt, oder
 - wenn es eine verbindliche Rechtsnorm gibt, die eine Verarbeitung regelt, oder
 - wenn der Betroffene einer Verarbeitung seiner Daten ausdrücklich zustimmt.

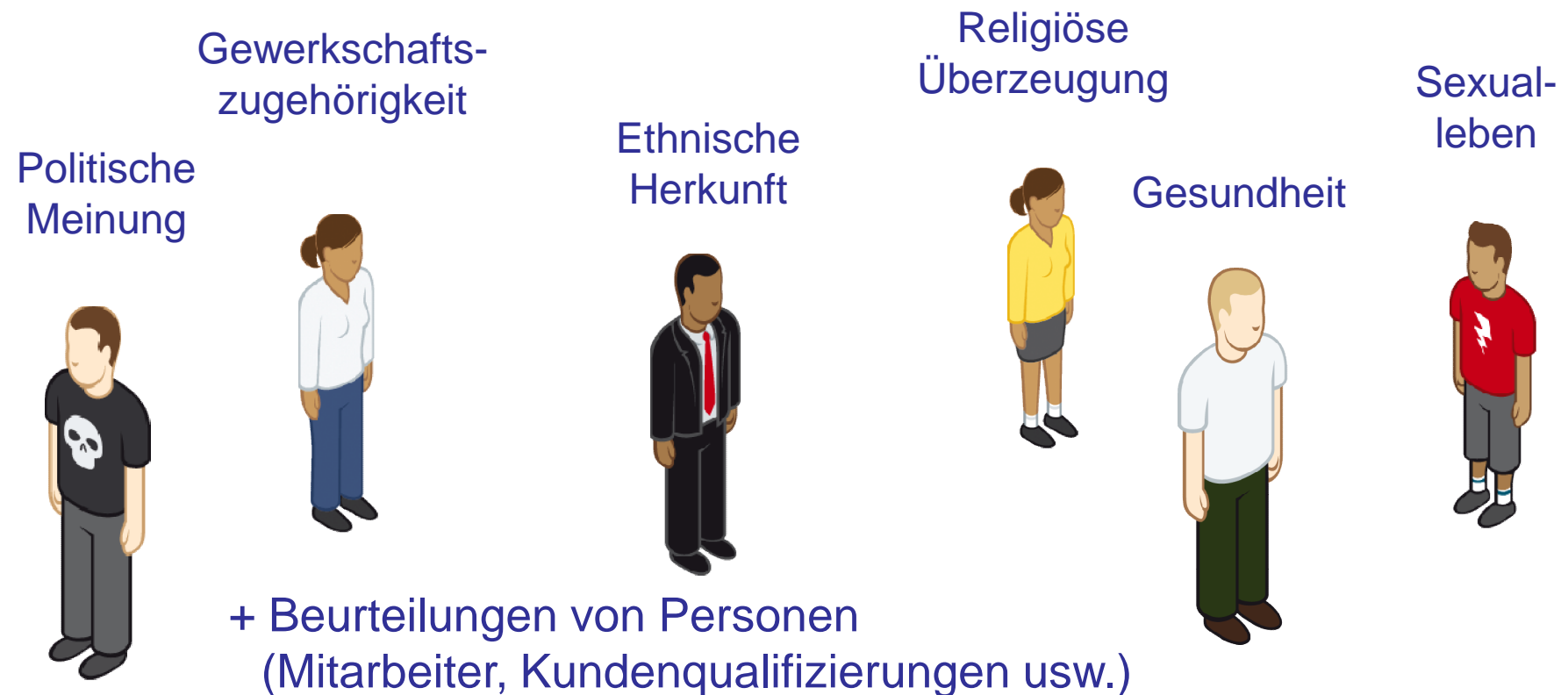
Personenbezogene Daten

= Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person (Betroffener)



"sensible" personenbezogene Daten

Strengere Regeln gibt es lt. Gesetz für den Schutz von **besonderen Arten** personenbezogener Daten – sie sind **besonders schützenswert**



Verpflichtung auf das Datengeheimnis

- Den bei der Datenverarbeitung (sehr weit zu fassen!) **beschäftigten Personen** ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). → § 5 BDSG
- Diese Personen **sind**, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit **auf das Datengeheimnis zu verpflichten**. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.
- **Ordnungswidrig** handelt unter anderem, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Es droht Geldbuße bis 300.000 Euro.
- Wer eine solche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.
- **Die Verpflichtung** ist per Unterschrift durch den Verpflichteten (Mitarbeiter/in) zu bestätigen.

Beschäftigte sind ...

1. **Arbeitnehmerinnen und Arbeitnehmer,**
2. **zu ihrer Berufsbildung Beschäftigte** (Ausbildung, Fortbildung, Umschulung, Ausbildungsvorbereitung)
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden)
4. **in anerkannten Werkstätten für behinderte Menschen Beschäftigte,**
5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte (freiwilliges soziales Jahr),
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten (freie Mitarbeiter usw.),
7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist (auch Rentner, frühere Beschäftigte)
8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Hier sind also auch arbeitnehmerähnliche Personen einbezogen – es geht dem Gesetzgeber also um das Schutzbedürfnis, nicht um den Status als AN

→ § 3 Abs. 11 BDSG

Folgen bei Datenschutzverletzungen

- **Missbrauch von personenbezogenen Daten** kann eine strafbare Handlung sein
(Konsequenzen je nach Schwere der Datenschutzverletzung)
- **Folgen für Mitarbeiter**
bis hin zur Abmahnung, Entlassung, Schadensersatz, Geldstrafen, Freiheitsstrafen
- **Folgen für das Unternehmen**
Imageverlust, finanzielle Einbußen, Prozesskosten, Schadensersatz

Arbeitnehmerdatenschutz ...

Beispiele für die Relevanz der Überprüfung von Arbeitnehmerdatenschutz:

- Erheben und Speichern von Beschäftigtendaten
- Biometrische Verfahren
- Videoüberwachung
- Ortung von Außendienstmitarbeitern
- Privatsphäre und Konsumverhalten
- Datenerfassung für Rufbereitschaft
- Entgeltabrechnung
- Arbeitszeit und Arbeitsverhalten
- Potenzialanalysen
- Gesundheitsdaten beim Wiedereingliederungsmanagement
- Technische Mittel wie Navi, RFID-Transponder in Firmenausweisen, Mobiltelefone, E-Mails usw.
- Private Nutzung von Internet und E-Mail
- ...

Begriffe zum Datenschutz (I)

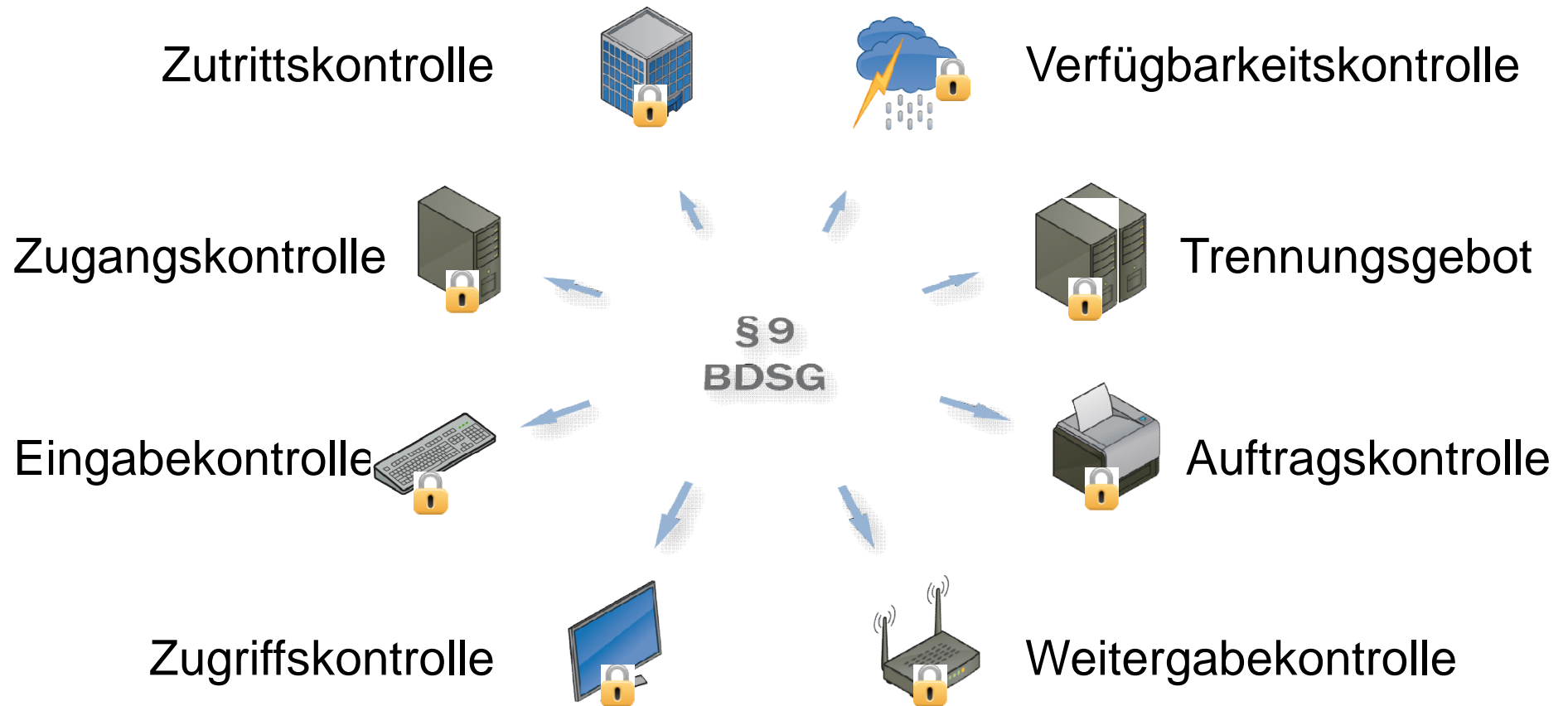
- Personenbezogene Daten = Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener)
 - Erheben = Beschaffen von Daten über Betroffene
 - Verarbeiten = Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten
 - Nutzen = jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt
- Nicht zu den personenbezogenen Daten gehören technische Daten oder Verfahrensbeschreibungen

Begriffe zum Datenschutz (II)

- **Speichern** = Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zur weiteren Verarbeitung oder Nutzung - Beispiel
- **Verändern** = inhaltliches Umgestalten gespeicherter personenbezogener Daten - Beispiel
- **Übermitteln** = Bekannt geben gespeicherter personenbezogener Daten an einen Dritten - Beispiel
- **Sperren** = Kennzeichnen personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken - Beispiel
- **Löschen** = Unkenntlich machen gespeicherter personenbezogener Daten – Beispiel
- **Anonymisieren** = Verändern personenbezogener Daten, so dass Angaben einer bestimmten Person nicht mehr zugeordnet werden können
- **Pseudonymisieren** = Ersetzen von Daten durch Kennzeichen, um die Bestimmung des Betroffenen auszuschließen oder zu erschweren
- **Verantwortliche Stelle** = wer personenbezogene Daten erhebt, verarbeitet oder nutzt oder dies in Auftrag gibt

Grundprinzipien des Datenschutzes

technische und organisatorische Maßnahmen



Datenschutz - Datensicherheit



Meldepflicht seit 01. April 2010

Art der Daten: besondere personenbezogene Daten, Bankdaten, Kreditkartendaten, Gesundheitsdaten usw.

Vorfall: Daten sind Dritten unrechtmäßig zur Kenntnis gelangt bzw. es könnte so sein (Beispiel: Diebstahl eines Notebooks, Listen werden versehentlich an einen falschen Verteiler geschickt, ein USB-Stick geht verloren usw.)

Folge: die Aufsichtsbehörde ist umgehend zu informieren. Wenn polizeiliche Ermittlungen nicht mehr gefährdet sind, sind die Betroffenen, deren Daten verschwunden sind, ebenfalls zu informieren. Entstehen Schäden, ist das Unternehmen zum Ersatz des Schadens verpflichtet.

Ist das wegen der Vielzahl der Fälle nicht möglich, ist in zwei deutschlandweit erscheinenden Tageszeitungen eine mindestens halbseitige Anzeige zu schalten.

Folge: ein mehr als peinlicher Imageverlust für das Unternehmen

Vorbeugen: besondere Schutzmaßnahmen einleiten:

bei Notebooks (z.B. Festplattenverschlüsselung),

bei Speichermedien (Verschlüsselung),

bei Aktenentsorgung (Dienstleister sorgfältig auswählen) usw.

Hier tragen alle Mitverantwortung!

Handreichungen zum Datenschutz I

1. Es dürfen nur solche personenbezogenen Daten verarbeitet werden, die **unbedingt erforderlich** sind. "Nice to have" als Begründung für Daten reicht nicht aus.
2. Es dürfen keine personenbezogenen Daten zur Einsicht **offen da liegen**, wenn Unbefugte (Externe und Interne) diese einsehen könnten. Dies betrifft offene Schriftstücke in Ablagekörben und Druckern, auf Schreibtischen, Büromöbeln, Fenstersimsen, Bildschirmen usw. gleichermaßen. Im Zweifelsfall Unterlagen umdrehen, wegschließen, Bildschirmschoner einschalten oder ähnliche geeignete Maßnahmen ergreifen. Das Büro ist beim Verlassen zu verschließen, wenn Unterlagen unverschlossen daliegen.
3. **Personenbezogene Unterlagen** dürfen **nicht** über den Papierkorb entsorgt werden. Dafür gibt es eigene Datenschutzboxen und / oder Shredder.
4. Es dürfen grundsätzlich keine personenbezogenen Daten per **E-Mail, Fax, Post** oder auf anderem Weg übermittelt werden, wenn der Betroffene (um dessen Daten es sich handelt) nicht zugestimmt hat – es sei denn, die Übermittlung ist vom Datenschutz her sowohl unbedenklich als auch für den Fortgang der Arbeit erforderlich.
5. Sie sollten keine E-Mail-Verteiler verwenden, die **mehr als drei** offen einsehbare Empfänger haben; ansonsten verwenden Sie die Funktion "Bcc bzw. "Blindkopie" - prüfen Sie aber in jedem Fall, ob wirklich alle Empfänger die Daten erhalten müssen.

Handreichungen zum Datenschutz II

6. Sensible Daten dürfen **nur verschlüsselt** versendet werden.
7. Außerhalb des Unternehmens darf mit niemandem über personenbezogene Daten gesprochen werden. Innerhalb nur über solche, die von Kollegen unbedenklich eingesehen werden dürfen.
8. Private Hard- und Software darf im Unternehmen **nur mit ausdrücklicher Erlaubnis** eingesetzt werden. Dies gilt ganz besonders für private USB-Sticks. Das bedeutet auch: keine Daten aus dem Unternehmen mitnehmen, es sei denn, es ist abgesprochen oder ein Vorgesetzter hat das angeordnet.
9. Der Datenschutz sollte **nicht** als **Schutzbehauptung** vorgeschoben werden, wenn man zwar Auskunft erteilen soll und darf, aber keine Lust dazu hat.
10. Der Datenschutzbeauftragte sollte ernst genommen werden. Er will Ihnen keine Schikanen aufbrummen, sondern mit Ihnen zusammen Schaden für das Unternehmen vermeiden. Haben Sie Vertrauen zu ihm und fragen oder **informieren Sie ihn**, wenn Ihnen hinsichtlich Datenverarbeitung oder -übermittlung etwas **seltsam** vorkommt.

Vielen Dank für Ihre Aufmerksamkeit !

Thorsten Jordan

externer Datenschutzbeauftragter (IHK)

TeamDatenschutz
Wichernstraße 2
76185 Karlsruhe
Tel. 0721/5687870
Fax 0721/5687868

t.jordan@team-datenschutz.de
www.team-datenschutz.de