Bürgerrechte in der digitalen Gesellschaft und Folgen für den Beschäftigtendatenschutz

in der Tagung

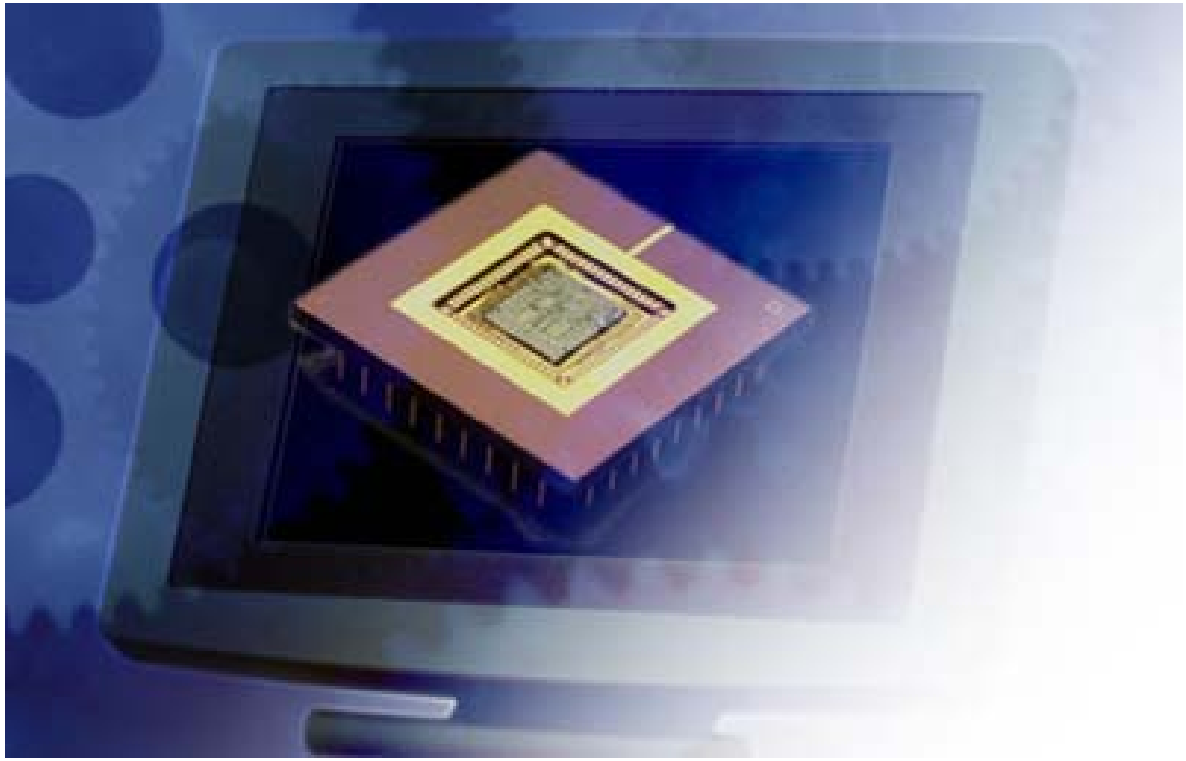
„Verlage, Rundfunk, Internet – Die Zukunft der Medien aus Sicht der Beschäftigten“

Lage-Hörste, 21. - 23.10.2011

Referent: Norbert Warga

GDD CERT. DATENSCHUTZ-BEAUFTRAGTER
GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERUNG e.V.

ver.di-Institut für Bildung, Medien und Kunst
Teutoburger-Wald-Str. 105
32791 Lage-Hörste
Telefon 05232/983-0
Fax 05232/983–462
E-Mail bst.lage-hoerste@verdi.de



1 Inhalt

2 „TROJANER“ in Betrieben und Behörden

Überwachungsmöglichkeiten mittels:

- ☐ Zeiterfassungssysteme (Arbeitszeit-, Gleitzeitdaten u.a.?)
- ☐ Bewegungssysteme und Zugangskontrollen
- ☐ Biometrische Datenerfassung
- ☐ Namensschilder
- ☐ Videoüberwachung
- ☐ Telefondatenerfassung
- ☐ Callcenter
- ☐ Unternehmensnetzwerk/e
- ☐ Internet, Intranet, Extranet, E-Mail
- ☐ Weitergabe von Personaldaten an Dritte
- ☐ Veröffentlichung von Arbeitsergebnissen, Bestenlisten

3 Daten in sozialen Netzen

Soziale Netzwerke – aber „das Böse lauert immer und überall …“

Auszüge aus AiB-Schwerpunktheft "Betriebsrat und neue Entwicklungen im Internet", Mai 2011 - "DER KOMMENTAR" von Norbert Warga

Soziale Netzwerke wachsen und ermöglichen immer mehr:

- **Begehrlichkeiten,**
- **Hoffnungen,**
- **Resonanzen,**
- **Gewinne,**
- **Botschaften,**
- **Meinungen,**
- **Schnüffeleien,**
- **Überwachungen,**
- **Enttäuschungen,**
- **Persönlichkeitsverletzungen,**
- **Datenschutzrechtsverstöße und**
- **Straftaten.**

- Soziale Netzwerke der Informationstechnik sind kein virtuelles Computerspiel sondern Elemente der realen Welt.
- Die reale Welt ist im Netz, das Netz ist real und dabei brutal für Verlierer und ertragreich für die Betreiber kommerzieller Netzdienste und diese nutzender Unternehmen.
- Ein Netz wie z.B. ein Fischer- oder Einkaufsnetz besteht aus geknoteten Fäden. IT-Netze sind ähnlich, es gibt es Knoten (Akteure: Personen, Institutionen, Firmen etc.) und (Verbindungs-)Linien zwischen diesen, den sog. Kanten.
- Dies erinnert an ein früheres Verfahren in der Bildungsarbeit: Dabei wurden Linien zwischen den Teilnehmern gezogen, die die Redebezüge zueinander darstellten und ggfls nummeriert einen Kommunikationsverlauf protokollierten. Dabei wurden die Aktivität eines Einzelnen, die Beziehungen einzelner sowie Gruppenbildungen und Prozessentwicklungen auf einem Blatt Papier deutlich und nachvollziehbar.
- Bezogen auf die IT-Kommunikation in einem Unternehmen würde dies aber rechtswidrig (vgl. Telekommunikationsgeheimnis Art. 10 GG, Art. 8 EMRK, § 88 TKG und § 206 StGB) dazu dienen, Kommunikationsprofile zu bilden und interaktive Prozesse der Beschäftigten abzubilden.

- Für die kommerziellen Netze sind die Auswertungen sowohl für das Verhalten, die Ansichten und Interessen der Einzelnen als auch deren Beziehungen von Interesse. Dies nimmt mit den Bedeutungen der Einzelnen für das Netz, dessen Wachstum und Attraktivität zu. Auch hier gilt, dass das Ganze mehr ist als die Summe seiner Teile (Aristoteles 384 – 322 v. Chr.).
- Datenschutzrechtlich sind die fehlenden Zwecke der Datenerhebung und Nutzung als Ordnungswidrigkeit und wegen des Vorsatzes und der Gewinnerzielungsabsicht als strafbare Handlungen von den Aufsichtsbehörden zu prüfen und wohl auch nach deren eigenen Bekunden zu werten (vgl. Peter Schaar in Facebook ohne Datenschutz?)
- Facebook mit Sitz in USA bietet Webdienste für soziale Netzwerke mit einem Mitgliederbestand von 664,6 Mio. aktiver Nutzer (Social Media Schweiz. v. 6. April 2010 nach wikipedia). In Deutschland nutzen 23 Mio. Besucher Facebook Social Network (nach http://www.socialmediaschweiz.ch/html/deutschland.html - Abruf 20.10.2011).
- Damit ist Facebook nach YouTube auf Platz 2 und hat als **Datenkrake den Negativpreis „Big Brother Awards 2011“** erhalten – herzlichen Glückwunsch!

Angesichts der reichhaltigen Kritiken wie z.B.:

- **Ausspionieren von fremden e-Mail-Kontakten (hallo Chef – Sie auch hier?),**
- **Offenlegen privater Daten bei Kenntnis der E-Mail-Adresse,**
- **Verwendung und Weitergabe aller Nutzerdaten zu Werbezwecken,**
- **Erhebung von Kommunikationsdaten von Nichtmitgliedern,**
- **Auswertungen von Nachrichtendiensten und Polizei,**
- **extremistische Inhalte und**
- **Weitergabe der Benutzeridentitäten durch Facebook-Applikationen**

war der Preis nicht nur verdient, sondern auch ein deutlicher Appell an die Datenschutzbehörden.

Neue Mobbingvariante: Cybermobbing

FOTO von Joel Horn

siehe http://www.woman.at/articles/1032/558/275392/facebook-jo-l-tod-michaela-horn-schicksal

„Facebook hat Joël in den Tod getrieben“ –

Michaela Horn … Cyber-Mobbing führte zum Selbstmord

Ein 13-jähriger wurde in der Schule und im Internet gemobbt: So wollte Joël nicht mehr leben! Er beging Selbstmord!

WOMAN 13.08.2010 Abruf 20.10.2011 http://www.woman.at/articles/1032/558/275392/facebook-jo-l-tod-michaela-horn-schicksal

4 Informationelle Selbstbestimmung

Grundrecht abgeleitet aus Art. 2 Abs. 1
i.V. mit Art. 1 Grundgesetz
Bundesverfassungsgericht 1983:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, **wer was wann und bei welcher Gelegenheit** über sie weiß.“

5 Rechtsquellen des Datenschutzes

Verfassungsrecht Grundgesetz (GG)

Art. 1 (1) [1]Die Würde des Menschen ist unantastbar. [2]Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Art. 2 (1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Allgemeine Datenschutzgesetze

Bundesdatenschutzgesetz (BDSG)

Bundesbehörden / nicht-öffentlicher Bereich (z.B. Wirtschaft, e.V.)

16 Landesdatenschutzgesetze

Landesbehörden, Kommunale Behörden

Bereichsspezifische Datenschutzgesetze

z.B. SGB X, TMG, TKG, Polizeigesetze, Rundfunkgesetze

Besondere arbeitsrechtliche Regelungen zu personenbezogenen Daten

Dienstvereinbarungen mit normativer Wirkung im Arbeitsvertrag

6 Medienprivileg im Datenschutzrecht
§ 41 BDSG Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

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

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

(3) [1]Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der

Berichterstattung zu Grunde liegenden, zu seiner Person gespeicherten Daten verlangen. [2]Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

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

[3]Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) [1]Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. [2]An Stelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

7 § 57 RStV - Datenschutz bei journalistisch-redaktionellen Zwecken

Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag - RStV -)

(1) Soweit Unternehmen und Hilfsunternehmen der Presse als Anbieter von Telemedien personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken erheben, verarbeiten oder nutzen, gelten nur die **§§ 5, 7, 9 und 38a des Bundesdatenschutzgesetzes mit der Maßgabe, dass nur für Schäden gehaftet wird, die durch die Verletzung des Datengeheimnisses nach § 5 des Bundesdatenschutzgesetzes oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des § 9 des Bundesdatenschutzgesetzes eintreten.** Besondere staatsvertragliche oder landesrechtliche Bestimmungen für den Rundfunk bleiben unberührt.

(2) Werden über Angebote personenbezogene Daten von einem Anbieter von Telemedien ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet und wird der Betroffene dadurch in seinen schutzwürdigen Interessen beeinträchtigt, kann er **Auskunft** über die zugrunde lie-

genden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit durch die Mitteilung die journalistische Aufgabe des Veranstalters durch Ausforschung des Informationsbestandes beeinträchtigt würde oder aus den Daten

1. auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung mitgewirkt haben oder

2. auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Miteilungen für den redaktionellen Teil

geschlossen werden kann. Der Betroffene kann die Berichtigung unrichtiger Daten oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Die Sätze 1 bis 3 gelten nicht für Angebote von Unternehmen und Hilfsunternehmen der Presse, soweit diese der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserates unterliegen.

(3) Führt die journalistisch-redaktionelle Verwendung personenbezogener Daten zur Verbreitung von Gegendarstellungen des Betroffenen oder zu Verpflichtungserklärungen, Verfügungen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, sind diese Gegendarstellungen, Unterlassungserklärungen oder Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

8 Verantwortliche Stelle

§ 3 Absatz 7 BDSG

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.

Bedeutung?

Wann sind Abteilungsleiter und
wann Beschäftigte
„verantwortliche Stelle“ i.S. des Gesetzes?

9 Personenbezogene Daten

sind

Einzelangaben **über**

persönliche **oder**

sachliche **Verhältnisse einer**

bestimmten **oder**

bestimmbaren natürlichen Person

(Betroffener).

§ 3 Abs. 1 BDSG, „Weitere Begriffsbestimmungen“

10 Bedeutung für Beschäftigungsverhältnisse

Personaldaten

gesetzliche Auskunfts-

und Meldepflichten

(DEÜV)

Betriebs- Geschäftsdaten

Wann werden

Betriebs-, Geschäftsdaten

zu Personaldaten?

11 Bundesdatenschutzgesetz (Novelle II) 2009

in Kraft am 1. September 2009

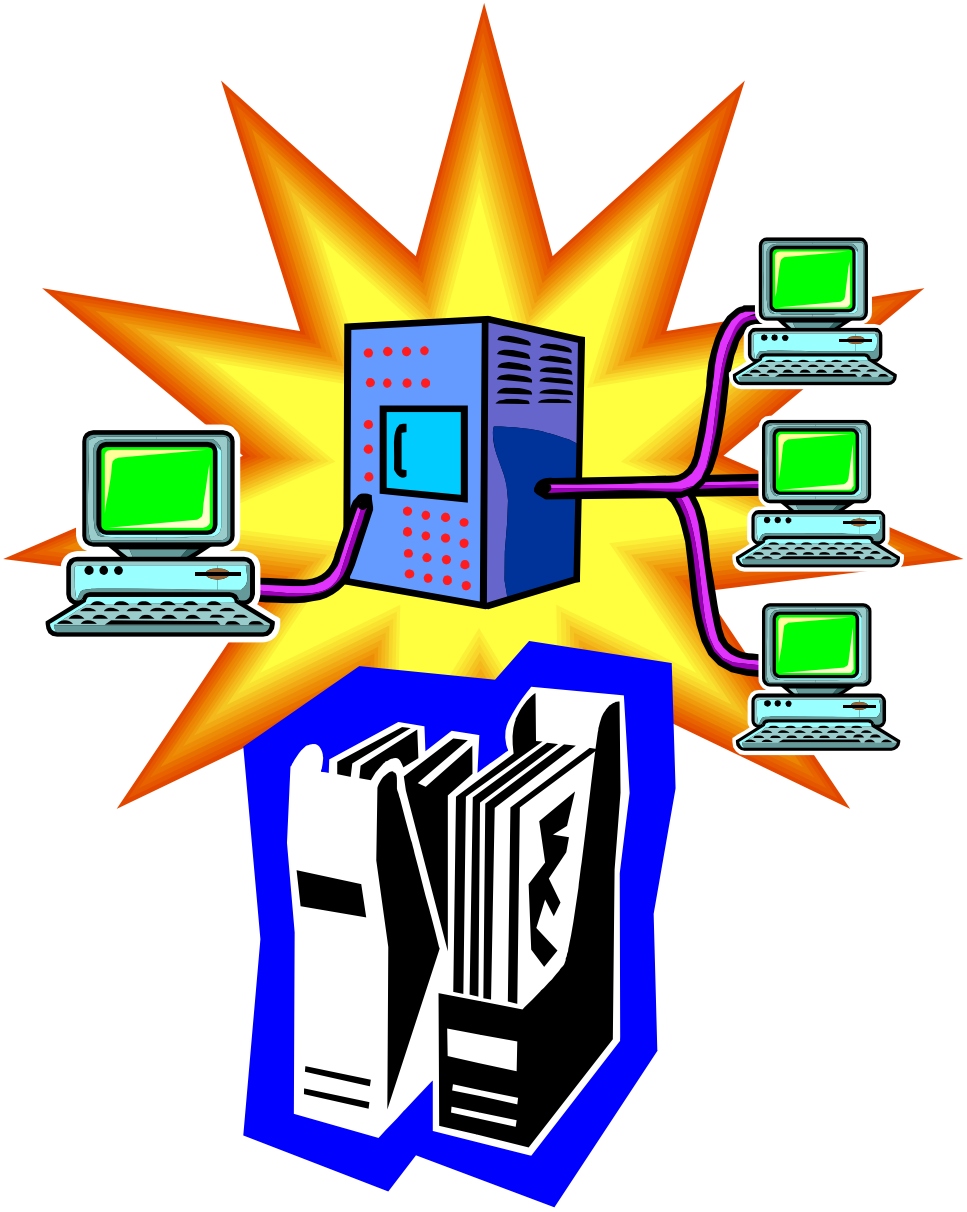
Bestimmungen der europäischen Datenschutzrichtlinie 95/46/EG vom Oktober 1995 in der Bundesrepublik als nationales Recht

Die Vorschriften des BDSG finden im nicht-öffentlichen Bereich für jede Verarbeitung personenbezogener Daten Anwendung.

Altes Recht benannte bis 2001 positiv die Tätigkeiten, bei denen das Bundesdatenschutzgesetz zur Anwendung gelangte;

Es sind nur Datenverarbeitungen von dem Anwendungsbereich ausgeschlossen, die lediglich von einer „natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen werden“.

Alle übrigen Datenverarbeitungen durch nicht-öffentliche Stellen automatisierte Verarbeitungen oder nicht-automatisierte Dateien § 1 Abs. 2 Nr. 3 BDSG.



Und seit 1.09.2009 personenbezogene nicht-automatisierte Daten der Beschäftigten § 32 Abs. 2 BDSG

12 Zweckbindungsgrundsatz

Strikte Geltung

- **sowohl bei der Datenverarbeitung für eigene Zwecke**
- **als auch bei geschäftsmäßiger Datenverarbeitung;**
- **bereits bei der Erhebung personenbezogener Daten;**

§ 28 BDSG Datenerhebung, -verarbeitung u. -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 für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das

schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Im BayDSG ist die Zweckbestimmung mehrfach gefordert.

§ 3 (11) BDSG Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer
2. zu ihrer Berufsbildung Beschäftigte
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,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 3a BDSG Datenvermeidung und Datensparsamkeit

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

§ 32 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.

12.1 Art. 15 BayDSG Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(7) [1]Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben, ist über die Vorschriften dieses Abschnitts hinaus nur zulässig, wenn

8. es erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts Rechnung zu tragen, oder

Besonders sensible Daten nach § 3 Abs. 9 BDSG / Art 15 Abs. 7 BayDSG „besondere Kategorien personenbezogener Daten“

- ☐ rassische und ethnische Herkunft
- ☐ politische Meinungen (z.B. Partei, Wählerverhalten)
- ☐ religiöse oder philosophische Überzeugungen (z.B. Kirchenzugehörigkeit)
- ☐ Gewerkschaftszugehörigkeit
- ☐ Gesundheit (z.B. ärztl. Gutachten, Krankschreibungen)
- ☐ Sexualleben

13 Schutzstufenkonzept

oder:

Sind alle Daten gleich?

Zu welcher Schutzstufe gehören die personenbezogenen Daten Ihrer Kunden, Bürger oder Beschäftigten?

Konferenz der Datenschutzbeauftragten des Bundes und der Länder + BSI:

- **Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten.**
- **Die Betrachtung ist vielmehr auf die gesamte Datei, ggf. auch auf die unmittelbar verknüpfbaren Datenbestände auszudehnen.**

Stufe A:	**frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z.B. Adressbücher, Benutzerkataloge in Bibliotheken,**
Stufe B:	**personenbezogene Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. beschränkt zugängliche öffentliche Dateien**
Stufe C:	**personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann ("Ansehen"), z.B. Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten.**

Stufe D:	**personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann ("Existenz"), z.B. Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Konkurse,**
Stufe E:	**Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z.B. Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.**

Falls die Sensibilität nicht bekannt ist, ist von der höchsten Sensibilitätsstufe auszugehen!

Denkbar ist auch, dass der Schutz empfindlicher Firmendaten die Einstufung bestimmt.

13.1 Schutz vor Ordnungswidrigkeiten, Bußgeldern, strafbaren Handlungen und Schadensersatzansprüchen

Einen **Straftatbestand nach § 203 StGB** begehen Datenverarbeiter, wenn sie unbefugt Daten offenbaren, die ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis beinhalten, das ihnen als

- **Amtsträger,**
- **für den öffentlichen Dienst besonders Verpflichteten,**
- **Person, die Aufgaben / Befugnisse nach dem Personalvertretungsrecht wahrnimmt, (Betriebsräte § 120 BetrVG)**
- **Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörige eines anderen Heilberufs,**
- **Berufspsychologen,**

- **Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,**
- **Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle,**
- **Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,**
- **staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen,**
- **Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle,**
- **Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates,**

das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates oder

- **öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist,**
- **Beauftragter für den Datenschutz**

anvertraut worden oder sonst bekannt geworden ist. Das Strafmaß ist Freiheitsstrafe bis zu einem Jahr oder Geldstrafe. Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder zu schädigen oder das Geheimnis also die Daten zu verwerten, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe (vgl. § 203 Abs. Abs. 5 und § 204 Abs. 1 StGB).

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten *(Datenpannen)*

Stellt eine nicht öffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz9),

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder

4. personenbezogene Daten zur Bank- und Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen.

Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten.

Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten.

Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hin-

sichtlich der Information der Betroffenen gleich geeignete Maßnahme.

Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

13.2 § 43 Bußgeldvorschriften

§ 43 Bußgelder

Die Bußgeldtatbestände wurden erweitert und das mögliche Bußgeld wurde erhöht:

- **Organisationsvergehen 25.000 zu 50.000 €.**
- **Materielle Vergehen 250.000 zu 300.000 €.**
- **Außerdem soll das Bußgeld den wirtschaftlichen Vorteil des Täters aus den Verstößen übersteigen, deshalb kann das Bußgeld in Einzelfällen die Höhe von 300.000 € überschreiten.**

13.3 Ordnungswidrigkeiten nach § 43 Abs. 2 Nr. 1-3 und Abs. 3 BDSG

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

…

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu **fünfzigtausend Euro**, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu **dreihunderttausend Euro** geahndet werden.
Die Geldbuße soll den **wirtschaftlichen Vorteil**, den der **Täter** aus der Ordnungswidrigkeit gezogen hat, **übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.**

13.4 § 44 BDSG Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche 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.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.

13.5 Weitere hier beachtliche Strafvorschriften

§ 201 Vertraulichkeit des gesprochenen Wortes

§ 201a Verletzung des höchstpersönl. Lebensbereichs durch Bildaufnahmen

§ 202a StGB Ausspähen von Daten

§ 204 StGB Verwertung fremder Geheimnisse, namentlich Betriebs- oder Geschäftsgeheimnis

§ 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses

§ 242 StGB Diebstahl und § 243 besonders schwerer Fall des Diebstahls

§ 263a Computerbetrug

§ 268 Fälschung technischer Aufzeichnungen

§ 269 Fälschung beweiserheblicher Daten

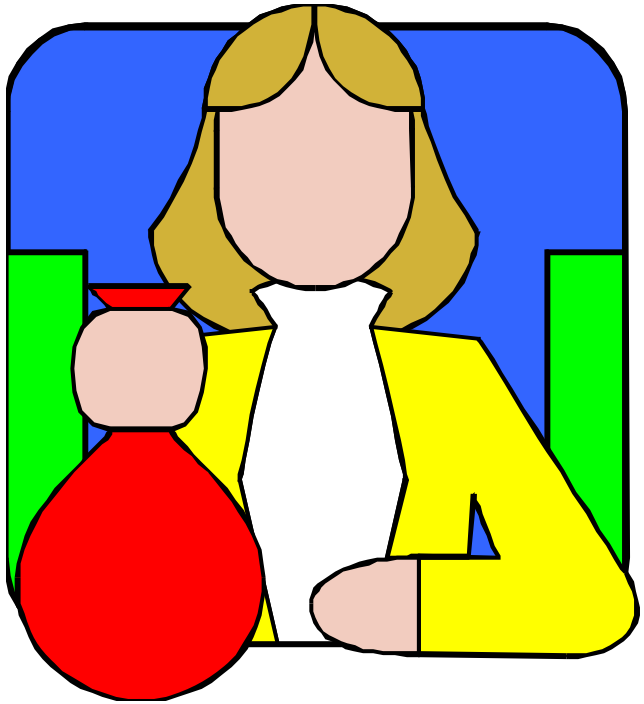
§ 303a Datenveränderung

§ 303b Computersabotage

§ 357 Verleitung eines Untergebenen zu einer Straftat
Strafmaße: 1 – 5 Jahre oder Geldstrafe

14 § 7 Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Daten-schutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet.



Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

15 § 823 BGB Schadensersatzpflicht

(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) 1Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. 2Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

16 § 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz **unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu**, ist ihr Träger dem Betroffenen **unabhängig von einem Verschulden** zum Schadensersatz verpflichtet.

(2) Bei einer **schweren Verletzung** des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der **nicht Vermögensschaden** ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130 000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

Die Ersatzpflicht entfällt,

soweit die verantwortliche Stelle

die nach den Umständen des Falles

gebotene Sorgfalt

beachtet hat.

§ 7 Satz 2 BDSG

Art 14 Abs. 1 Satz 2 BayDSG

17 Tabelle zu 8 Datenschutzanforderungen der Anlage zu § 9 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren **(Zutrittskontrolle),**
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können **(ZUGANGSKONTROLLE),**

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die **ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (ZUGRIFFSKONTROLLE),**

4. zu gewährleisten, dass personenbezogene Daten **bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung**

personenbezogener Daten durch Einrichtungen zur Datenüber-tragung vorgesehen ist

(WEITERGABEKONTROLLE),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Daten-verarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(EINGABEKONTROLLE),**

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftrag-gebers verarbeitet werden können **(*AUFTRAGSKONTROLLE*),**

7. zu gewährleisten, dass personenbezogene Daten gegen *zufällige* Zerstörung oder Verlust geschützt sind **(VERFÜGBARKEITSKONTROLLE),**

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können **(Trennungsgebot)**.

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

Für die Zugangs-, Zugriffs- und Weitergabekontrolle hat der Gesetzgeber die Verschlüsselung als geeignete Maßnahme bestimmt.

17.1 Verpflichtungen zur Einhaltung der IT -Richtlinien

- **Problem der fehlenden Rechtsvorschrift! –**
  Kann nur durch Betriebs-/Dienstvereinbarung geheilt werden!

- **Eine nur arbeitsvertragliche Verpflichtung wäre nach § 4a BDSG rechtswidrig.**

§ 4a BDSG:

(1) [1]**Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.** [2]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. [3]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [4]Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) [1]Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. [2]In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

17.2 Vorabkontrolle von Datenverarbeitungen

für Datenverarbeitungen,

die mit besonderen Risiken

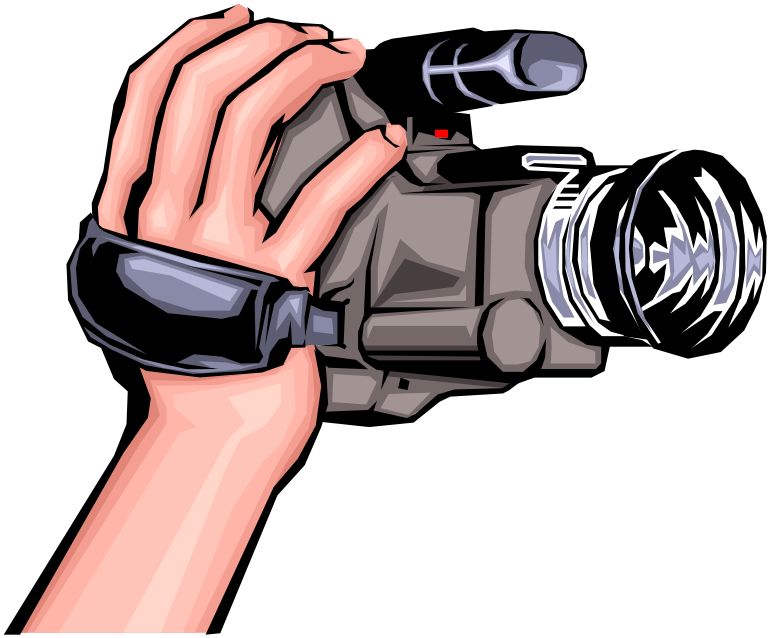
für das Persönlichkeitsrecht

verbunden sind. § 4d Abs. 5

Aufgabe des bDSB § 4d Abs. 6

Art. 26 BayDSG - Freigabe

18 Videobeobachtung



- **gesetzliche Vorgaben für die VIDEOBEOBACHTUNG öffentlich zugänglicher Räume, auch durch Private, § 6b BDSG**

nur noch in bestimmten Fällen zulässig,
durch geeignete Maßnahmen erkennbar zu machen & gegen schutzwürdige Interessen der Betroffenen abzuwägen.
Zweckbindung, Benachrichtigungs- und Löschungspflichten;

18.1 Videoüberwachung von Produktionsprozessen in Unternehmen - BAG zur verdachtsunabhängigen Videoüberwachung

- **Der Spruch einer Einigungsstelle zur Einführung einer Videoüberwachung in einem Berliner Briefverteilzentrum der Deutschen Post AG ist unwirksam. (Schichtbetrieb mit ca. 650 AN mit täglich ca. 2,5 Mio. Briefen, Verluste)**
- **Zur Reduzierung der Verluste plante die Arbeitgeberin die Einführung einer Videoüberwachung. Da der Betriebsrat seine Zustimmung verweigerte, rief sie die Einigungsstelle an. Deren Spruch sieht die dauerhafte Einrichtung einer Videoüberwachung durch in der Halle sichtbar angebrachte Kameras vor.**
- **Die Videoanlage soll verdachtsunabhängig wöchentlich bis zu 50 Stunden eingesetzt werden können. Für die Arbeitnehmer ist nicht erkennbar, wann die Anlage in Betrieb ist. Die Aufzeichnungen müssen in der Regel spätestens nach acht Wochen gelöscht werden.**
- **Der Betriebsrat hat den Einigungsstellenspruch gerichtlich angegriffen - beim Bundesarbeitsgericht hatte er Erfolg.**

- **Einerseits hat die Arbeitgeberin die Pflicht, für die Sicherheit des Briefverkehrs und des grundrechtlich geschützten Postgeheimnisses zu sorgen.**
- **Andererseits wird durch die Videoüberwachung erheblich in das ebenfalls grundrechtlich geschützte Persönlichkeitsrecht der Arbeitnehmer eingegriffen. Keiner dieser beiden Rechtspositionen gebührt absoluter Vorrang. Vielmehr ist eine auf die Umstände des jeweiligen Falles bezogene Abwägung erforderlich.**
- **Danach ist die dauerhafte, verdachtsunabhängige Videoüberwachung der Belegschaft des Berliner Briefzentrums unter den vorliegenden Umständen unverhältnismäßig.**
  BAG Beschluss vom 29. Juni 2004 - 1 ABR 21/03 -

18.2 Video-Überwachung bei Unterschlagungsverdacht

- **Hat der Arbeitgeber nur durch den Einsatz von heimlicher Video-Überwachung die Möglichkeit, einem verdächtigten Mitarbeiter Unterschlagung nachzuweisen, ist diese Überwachung trotz Eingriff in das Persönlichkeitsrecht der Gefilmten (mögliche Nichtigkeit der Beweise) rechtens.**
- **Allerdings dürften sie berücksichtigt werden, wenn besondere Umstände dies erfordere und die Verhältnismäßigkeit gewahrt bleibe.**
- **In diesem Fall hatte der Arbeitgeber einen schwerwiegenden Verdacht gegen die Klägerin, den er nicht mit anderen Mitteln hätte belegen können, die die Persönlichkeitsrechte der Frau gewahrt hätten.**
- **Nur mittels der Video-Überwachung sei ein solcher Nachweis möglich geworden.**
  Bundesarbeitsgericht, Erfurt; Urteil vom 27.03.2003; Az.: 2 AZR 51/02

19 Telefondatenerfassung; private oder geschäftliche Telefonate

- **In welchem Umfang darf ein Unternehmen Aufzeichnungen von Gesprächsdaten zum Nachweis von Privatgesprächen auf Firmenkosten heranziehen bzw. welche Vorschriften sind datenschutzrechtlich zu beachten?**
- **Soweit ein Unternehmen die private Telefonnutzung zulässt, ist es Telekommunikationsdiensteanbieter und hat insbesondere das Fernmeldegeheimnis nach Maßgabe des § 88 Telekommunikationsgesetz (TKG) zu wahren.**
- **Eine Aufzeichnung der Kommunikationsdaten privater Telefonate der Beschäftigten ist dem Unternehmen ausschließlich zu Abrechnungszwecken erlaubt.**
- **Unterliegt die private Nutzung speziellen Einschränkungen, beispielsweise zeitliche Beschränkung auf Pausen o.ä., müssen die Beschäftigten sich ausdrücklich und individuell mit diesen Nutzungsbedingungen einverstanden erklären.**

- **Nur auf Basis einer derartigen Einwilligung ist ein Unternehmen in begründeten Verdachtsfällen berechtigt die sich aus der Abrechnung insgesamt ergebende Zeitdauer privater Telefongespräche auf die Vereinbarkeit mit arbeitsvertraglichen Pflichten hin zu überprüfen.**
- **Dienstgespräche hingegen können kontrolliert werden.**
- **Rechtsgrundlage für die Erhebung und Speicherung der Daten dienstlich veranlasster Telefonate der Beschäftigten einer Firma zu Kontrollzwecken ist § 28 Abs. 1 Satz 1 Nr. 1 des Bundesdatenschutzgesetzes (BDSG).**
- **Daneben ist bei der Erfassung von Daten der von den Beschäftigten geführten Telefongespräche – sofern im Unternehmen ein Betriebsrat vorhanden ist – die Mitbestimmungsvorschrift aus § 87 Abs. 1 Nr. 6 des Betriebsverfassungsgesetzes zu beachten.**
- **Grundsätzlich ist die Möglichkeit, mit der Telekommunikationsanlage Gebührenabrechnungen zu erstellen, ein Hilfsmittel zur Gebührenabrechnung und nicht ein Kontrollinstrument zur Überwachung der Telefonpraxis der Mitarbeiterinnen und Mitarbeiter.**

- **Das Unternehmen ist allerdings befugt, Angaben über Telefongespräche zu verarbeiten, die von Firmenanschlüssen aus geführt werden.**
- **Hierbei ist zu unterscheiden zwischen geschäftlichen und privaten Gesprächen:**
- **Da die Firmenleitung darüber zu wachen hat, dass mit den zur Verfügung stehenden Geldern wirtschaftlich und sparsam umgegangen wird, ist sie auch befugt, das Führen von Geschäftsgesprächen zu überprüfen.**
- **Dafür ist es zulässig, die Zielrufnummer vollständig zu erfassen. Jeder Arbeitnehmer und jede Arbeitnehmerin ist seiner beziehungsweise ihrer Firma zur Rechenschaft über die Führung der beruflich veranlassten Gespräche verpflichtet.**
- **Im Rahmen von Stichproben und bei einem begründeten Verdacht, dass unbefugt Privatgespräche auf Kosten des Unternehmens geführt werden, kann eine diesbezügliche Überprüfung der Telefondaten zulässig sein.**

- **Eine regelmäßige Auswertung der Telefondaten zur Überprüfung des allgemeinen Arbeitsverhaltens der Beschäftigten ist sowohl aus datenschutzrechtlicher Sicht als auch nach der Rechtsprechung der Arbeitsgerichte unzulässig.**
- **Da die ausgewiesene Telefonnummer auf die angerufene Person schließen lässt, ist von einer Speicherung der vollständigen Rufnummer auch bei beruflich veranlassten Gesprächen dann abzusehen, wenn der Beschäftigte, der das Gespräch führt, einer besonderen berufsbezogenen Schweigepflicht im Sinne von § 203 Strafgesetzbuch unterliegt.**
- **Ebenso wie bei privaten Telefongesprächen ist in diesen Fällen die gewählte Telefonnummer um mindestens die letzten zwei Ziffern zu kürzen. – reicht das aus?**
- **Werden die Gesprächsnachweise über private Telefongespräche zur Abrechnung an die Beschäftigten übersandt, hat dies in verschlossenen, persönlich adressierten Umschlägen zu geschehen.**

- **Die Speicherung der erfassten Telefondaten ist auf den Zeitraum zu beschränken, in dem in der Regel abrechnungstechnische Fragen geklärt werden können, üblicherweise genügt hierzu eine Speicherung von drei Monaten.**

- **In der Regel empfiehlt es sich, zur Erfassung der Telefondaten eine Betriebsvereinbarung mit dem Betriebsrat des Unternehmens zu vereinbaren, die die oben ausgeführten datenschutzrechtlichen Überlegungen und das Persönlichkeitsrecht der betroffenen Mitarbeiterinnen und Mitarbeiter berücksichtigt.**

20 § 88 TKG 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 Dienstean-bieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt

oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) ….

20.1 TKG - Arbeitsverhältnis

- Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird. (§1 I Satz 2 TMG
- Das Telekommunikationsgesetz und die Pressegesetze bleiben unberührt. (§1 III TMG)
- Die Datenschutzvorschriften des Abschnitt 4 des TMG gelten nicht „im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken“ (§ 11 I Nr. 1 TMG)
- Praxis: Verbot der privaten aktiven Nutzung aber personenbezogene dienstliche e-Mailadresse ermöglicht passive Nutzung
- Bei aktiver oder passiver privaten Nutzung wird der Arbeitgeber zum Anbieter und muss das Telekommunikationsgeheimnis beachten

- Journalistisch-redaktionelle Zwecke > § 57 RStV

20.2 Art. 10 GG

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) [1]Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. [2]Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

20.3 Art. 8 EMRK Recht auf Achtung des Privat- und Familienlebens

(1) **Jede Person** hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer **Korrespondenz**.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

20.4 Frankreich: eMail am Arbeitsplatz unterliegt Briefgeheimnis

- **Das Oberste Gericht (Kassationsgerichtshof) stellte fest, dass Arbeitgebern das Schnüffeln in den E-Mails ihrer Angestellten verboten ist. (7Jahre)**

- **"Mitte 1995 hatte Nikon France einem AN gekündigt, weil dieser während der Arbeitszeit am Computerarbeitsplatz private Angelegenheiten erledigt habe. (...) Zum Beweis legte Nikon France dem Gericht zahlreiche Dateien vor, die im Verzeichnis *Persönlich* im Arbeitsplatz-Computer des AN waren.**

- **(...) Unter Berufung auf die EU Menschenrechtskonvention (Art. 8) kam der Kassationsgerichtshof zu dem Ergebnis, dass hier eine gravierende Verletzung der privaten Sphäre des Arbeitnehmers vorliege. Auch am Arbeitsplatz und während der Arbeitszeit habe der Arbeitnehmer Anspruch auf den Schutz seines Privatlebens. Dazu gehöre vor allem der Schutz des Briefgeheimnisses.**

- **Dieser Schutz bleibt unangetastet, auch wenn der AG ausdrücklich die private Nutzung untersagt und der AN dieses Verbot nicht beachtet hat."**

Cour de cassation, Urteil Nr. 4164 vom 2.10.2001, AZ 99-42.942

Der Schutzbereich von Art 8 Abs 1 der Europäischen Menschenrechtskonvention im Fall (MRK) erfasst mit der Achtung von Privatleben und Korrespondenz auch die Nutzung von E-Mail und Internet am Arbeitsplatz. Das gilt auch für die Überwachung von Verkehrsdaten. Ein dem zuwider gerichtetes Handeln des Arbeitgebers berechtigt die/den Betroffene/n zum finanziellen Ersatz (hier 3.000,- €) des erlittenen immateriellen Schadens. Dies gilt ebenso für das Abhören privater Telefongespräche (Fall Halford 10.000,- £) der Arbeitnehmer durch den Arbeitgeber (Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil v. 03.04.2007 - 62617/00 – Lynette Copland gegen Vereinigtes Königreich – Juris; EuGRZ 2007, 415-420).

20.5 Kann einem Arbeitnehmer per E-Mail gekündigt werden?

- **In England hatte ein Arbeitgeber seinen mehreren tausend Mitarbeitern per SMS oder per E-Mail gekündigt. Ist dies in Deutschland auch möglich?**

- **Das Arbeitsgericht Frankfurt/Main glaubt das jedenfalls nicht.**

Eine per E-Mail geschriebene Kündigung ist nicht wirksam.

- **Eine Kündigungserklärung muss nach wie vor eigenhändig unterschrieben sein.**
  Arbeitsgericht Frankfurt/Main, AZ: 8 Ca 5663/00

20.6 Lesen von E-Mails in Spanien

- **Beschluss der „Audiencia Provincial de Madrid“ vom 20. September 2005 bestätigt Beschluss desselben Gerichts vom 23. Januar 2004.**

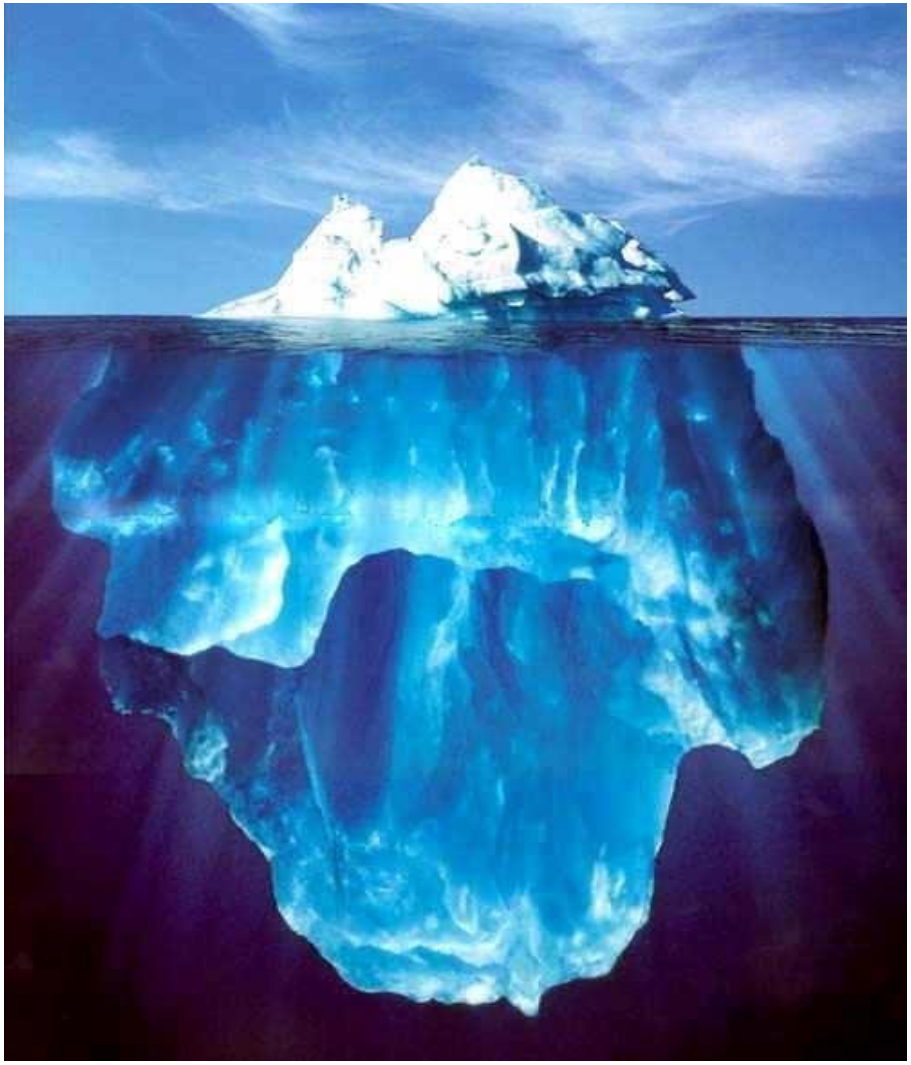
- **Demnach kann der Tatbestand des „Ausspähens von Geheimnissen“ („Descubrimiento de Secretos“, Código Penal, Art. 197.1) erfüllt sein, wenn der Arbeitgeber ohne Wissen des Arbeitnehmers ein Programm an dessen Arbeitsplatz installiert, durch das sämtliche ausgehende und eingehende Daten (einschließlich der privaten E-Mails) gespeichert und vom Arbeitgeber ausgespäht werden können.**

- **Die Straftat kann geahndet werden mit einer Gefängnisstrafe zwischen einem und vier Jahren oder in Form einer Geldstrafe mit Tagessätzen von einem Zeitraum zwischen 12 und 24 Monaten.**

21 Arbeitnehmerdatenschutz - Forderungen

Wachsende Bedeutung, gravierende Gefährdungen

- **Arbeitnehmerdatenschutz (ANDS): Es geht um ein Grundrecht**
- **Unversehrtheit, Respekt, Freiheit, Selbstbestimmung**
- **Gute Arbeit nicht ohne guten Datenschutz**
- **Datenskandale: Nur die Spitze des Eisberges**



Bedeutung und Gefährdung des Datenschutzes in der Arbeitswelt wurden in jüngster Zeit schlaglichtartig deutlich:

- Bespitzelungen bei der Telekom
- Screening bei der Bahn
- Videoüberwachung bei Lidl
- Detektiveinsätze bei Schlecker
- Krankendatensammlung bei der Post
- usw: www.datenschutzskandale.de

21.1 Forderungsaspekte zum Beschäftigtendatenschutz

- **Erweiterte Mitbestimmungsrechte von Betriebs- und Personalräten**
- **Konkrete Reglementierungen der AG-Kontrollmöglichkeiten**
- **Beschränkungen des Fragerechts von Arbeitgebern und Begrenzung ärztlicher Untersuchungen bei Einstellungen**
- **Klare Verbote, z.B. der heimlichen Überwachung von Beschäftigten, von Screenings, von Kontrollen mittels biometrischer Merkmale**
- **Schutz der persönlichen Daten vor unbefugtem Zugriff bei Verfahren wie der elektronischen Gesundheitskarte oder dem ELENA**

- **Besonderer Schutz von Beschäftigtendaten, wenn Beschäftigte gleichzeitig Kunden des Arbeitgebers sind**
- **Beweisverwertungsverbot für unzulässig erhobene Daten**
- **Härtere Sanktionen gegen Rechtsverstöße**
- **Einführung eines Verbandsklagerechts**
- **Regelungen zum grenzüberschreitender Datenaustausch**

22 Gesetzentwurf der Bundesregierung 21.09.2011

a) Nach der Angabe zu § 31 wird folgende Angabe eingefügt:

„Zweiter Unterabschnitt

Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“.

b) Die Angabe zu § 32 wird durch die folgenden Angaben ersetzt:

„§ 32 Datenerhebung vor Begründung eines Beschäftigungsverhältnisses

§ 32a Ärztliche Untersuchungen und Eignungstests vor Begründung eines Beschäftigungsverhältnisses

§ 32b Datenverarbeitung und -nutzung vor Begründung eines Beschäftigungsverhältnisses

§ 32c Datenerhebung im Beschäftigungsverhältnis

§ 32d Datenverarbeitung und -nutzung im Beschäftigungsverhältnis

§ 32e Datenerhebung ohne Kenntnis des Beschäftigten zur Aufdeckung und Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen im Beschäftigungsverhältnis

§ 32f Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch-elektronischen Einrichtungen

§ 32g Ortungssysteme

§ 32h Biometrische Verfahren

§ 32i Nutzung von Telekommunikationsdiensten

§ 32j Unterrichtungspflichten

§ 32k Änderungen

§ 32l Einwilligung, Geltung für Dritte, Rechte der Interessenvertretungen, Beschwerderecht, Unabdingbarkeit“.

In der
DV-LANDSCHAFT
ist
DATENSCHUTZ
UMWELTSCHUTZ!

23 Referent Norbert Warga

Datenschutzbeauftragter GDDcert, Dipl.-Sozialpädagoge;

Bis 07_2011 Gewerkschaft ver.di, Bundesvorstand in Berlin zuvor Gewerkschaft ÖTV, Hauptvorstand in Stuttgart

*GDD-zertifiziert (Gesellschaft für Datenschutz & Datensicherung e.V.)

- Wahrnehmung der gesetzlichen Aufgaben,
- DS-Beratungen, Seminare
- Projektberatungen, Projektleitung
- Beratungen partizipativer Beteiligung der Betriebs- und Personalräte in verschiedenen Fachbereichen bei Systemeinführungen und –änderungen (SAP (HR) HCM, LOGA, MetaDirectory etc.) sowie Internet, Intranet und Email
- Projektbeirat „JobCard“ des Bundesministeriums für Wirtschaft und Technologie und dessen Arbeitsgruppe Datenschutz (seit Jan. 2004 – 2011)

Referent, Sachverständiger zu:

- Personalplanung und Personalentwicklung für Betriebsräte und Personalräte (Seminarreihen des AiB-Verlages im Bund-Verlag)
- EDV-gestützte Personalwirtschaft (Bsp. SAP HCM, LOGA u.a.);
- Eingruppierungsrecht im ö.D., TVöD
- Datenschutz; Internet und Intranet; Netzwerke und Telekommunikation;

Veröffentlichungen:

KOMMENTAR BAYERISCHES PERSONALVERTRETUNGSGESETZ, wissenschaftl. Kommentar f. d. Praxis, Teil: Aufgaben, Beteiligungs-, Verfahrensrechte; Co-Autor Rudolf Aufhauser, Bund-Verlag 1988

2 LEHRSPIELFILME „Nicht ohne uns“ und „Die entscheidende Stimme“ jeweils zum Beschluss- und Einigungsstellenverfahren nach Betriebsverfassungs- und Personalvertretungsrecht, Hans Böckler Stiftung Düsseldorf 1988

KOMMENTAR LPVG BADEN-WÜRTTEMBERG; wissenschaftl. Kommentar f. d. Praxis, Teil: Aufgaben, Beteiligungs-, Verfahrensrechte; Co-Autor Rudolf Aufhauser u.a. Bund-Verlag 1990

KOMMENTAR LPVG SAARLAND, wissenschaftl. Kommentar f. d. Praxis, Teil: Aufgaben, Beteiligungs-, Verfahrensrechte; Co-Autor Rudolf Aufhauser, Arbeitskammer des Saarlandes 1991

PEP-SYSTEM, PC-Programm, Informationssystem für Betriebs-, Personalräte und Mitarbeitervertretungen; Idee, Konzept, Handbuch; Progr.: Glas und Programmierer des KRZN Moers 1991

GESTALTEN UND NUTZEN: Informations- und Kommunikationstechnik in den Handlungsfeldern einer kompetenten Betriebs- und Personalratsarbeit in Däubler, Bobke, Kehrmann, ARBEIT UND RECHT, Festschrift Albert Gnade, Bund-Verlag 1992

Das PERSONALRATSBÜRO, Organisationsplanung Arbeitsvorlagen, Kellner-Sachbuch-Verlag 1992

Einführung in das ARBEITS- UND SOZIALRECHT der Bundesrepublik Deutschland, 3. Auflage mit Lizenzausgaben der Bundeszentrale für politische Bildung, Teil: Konzeption, Sozialpolitik, Sozialversicherungsrecht; Erstauflage 1988, Co-Autoren Rudolf Aufhauser, Manfred Bobke von Camen, Bund-Verlag 1994

BAT-EINGRUPPIERUNGSRECHT, Kommentierung u. Arbeitshilfe, Teil: Konzept, Entwicklung des Tarifrechts, §§ 22, 23 a, 23 b BAT, Beteiligungsrechte Personal- u. Betriebsräte; Co-Autoren Stevens-Bartol, Fricke, Büttner-Verlag 1994

DATENSCHUTZ & DATENSICHERHEIT, Bundesdatenschutzgesetz 2001, ver.di 2002

Einführung in das ARBEITS- UND SOZIALRECHT der Bundesrepublik Deutschland, Bd 1 Arbeitsrecht in 111 Fragen und Antworten, Co-Autor R. Aufhauser, BOD 2003

Aktuelle Stellenbeschreibungen für ö.D. und Betriebe, Hrsg König/Schmidtke, Praxisleitfaden mit Software, FORUM-Verlag 2007 - 2010

Schutz & Sicherheit von Personaldaten, Büttner-Verlag 2008

Handbuch DIENSTVEREINBARUNGEN plus CD, Bund-Verlag 2009

KOMMENTAR BAYPVG, Basiskommentare Teil: Aufgaben, Beteiligungs-, Verfahrensrechte,1. - 6. Auflage, Co-Autor Rudolf Aufhauser, Bund-Verlag 2011

Kommunikation:

Badstr. 24, 82431
Kochel am See
Tel. 08851-7412
Fax 08851-7494
Mobil +49.171.5531724
norbert.warga@t-online.de