Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 1d)

Vorlesung im Sommersemester 2015

an der Universität Ulm

von Bernhard C. Witt

1. Grundlagen des Datenschutzes

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
✓	Technischer Datenschutz		Risiko-Management
➔	Mitarbeiterdatenschutz		Konzeption von IT-Sicherheit

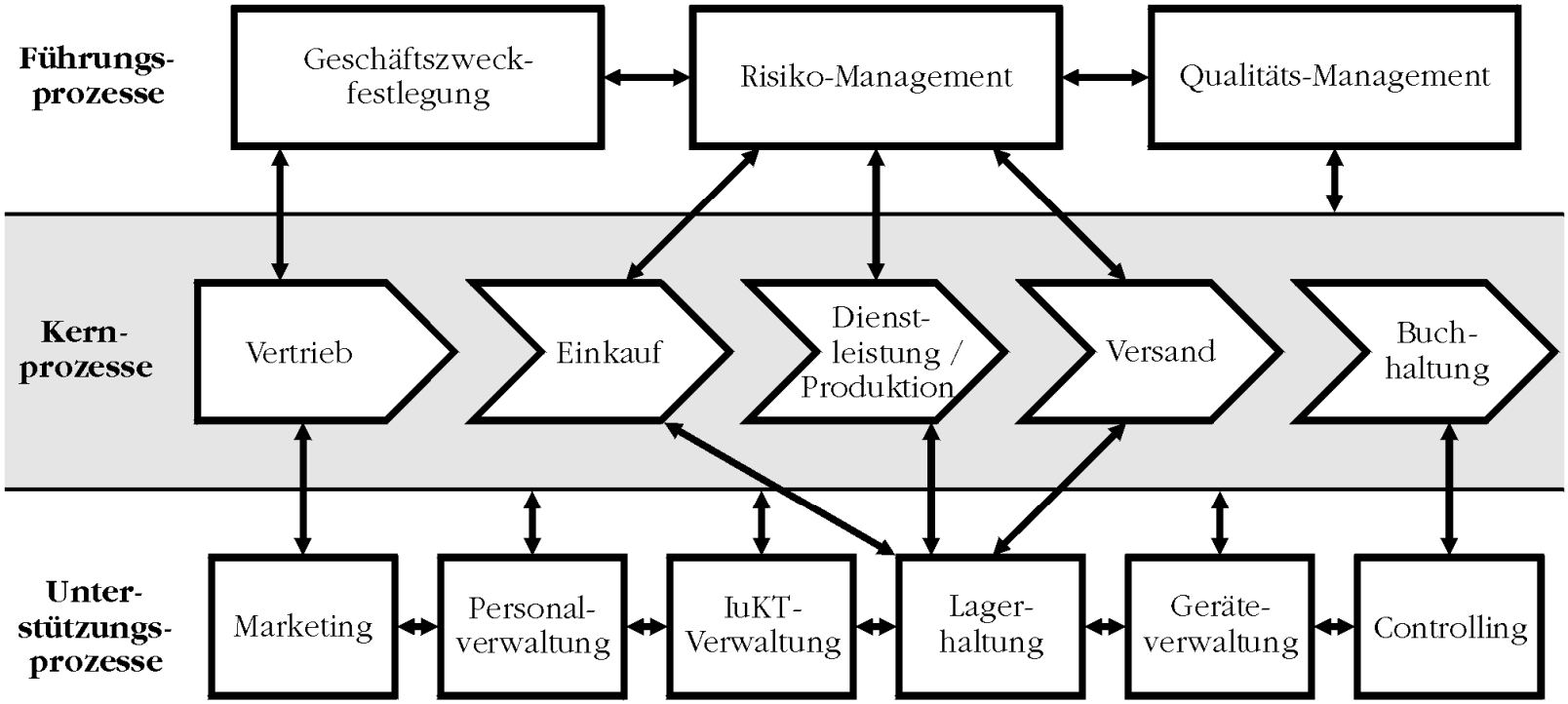
Mitarbeiterdatenschutz:

- Abgrenzung & Übersicht
  → **Details zu einzelnen Verfahren in der Übung!**
- Personalaktenführung
- Personaleinstellung
- Personaldatenverwaltung
- Mitbestimmung

Mitarbeiterdatenschutz

- Beim Mitarbeiterdatenschutz lassen sich 3 Phasen voneinander unterscheiden:
  1. Bewerbung & Einstellung eines Mitarbeiters
     → **Rechtsgeschäftsähnliches Schuldverhältnis** (Vorauswirkung)
  2. Vorgänge während der Beschäftigung
     → **Rechtsgeschäftliches Schuldverhältnis**
  3. Ausscheiden eines Mitarbeiters
     → **Rechtsgeschäftsähnliches Schuldverhältnis** (Nachwirkung)
- Beschäftigungsverhältnis erstreckt sich damit auf alle 3 Phasen
  → grundlegend: **§ 32 BDSG**; ergänzend § 28 Abs. 1 Nr. 2 BDSG sowie vorrangiges Bereichsrecht (u.a. Betriebsvereinbarungen, Anstellungsvertrag, Spezialrecht zur Arbeitszeitüberwachung & Videoüberwachung)
- **Leistungs- & Verhaltensbewertung** unterliegt Mitbestimmung, soweit ein Betriebsrat / Personalrat eingerichtet wurde, und der Vorabkontrolle durch den Datenschutzbeauftragten
- **Fähigkeitsbewertung** unterliegt „nur“ der Vorabkontrolle

Unternehmensprozesse



Datenschutzrechtliche Verfahren

Mitarbeiterdatenschutz

- Bewerbungsverfahren
- Personalaktenführung
- Arbeitszeitüberwachung
- Verwaltung des Personaleinsatzes
- Personalentwicklungsplanung
- Lohn- und Gehaltsabrechnung
- Elektronische Kommunikation
- plus ggf. weiterer, spezifischer Verfahren (z.B. zur Videoüberwachung, Qualitätskontrolle…)

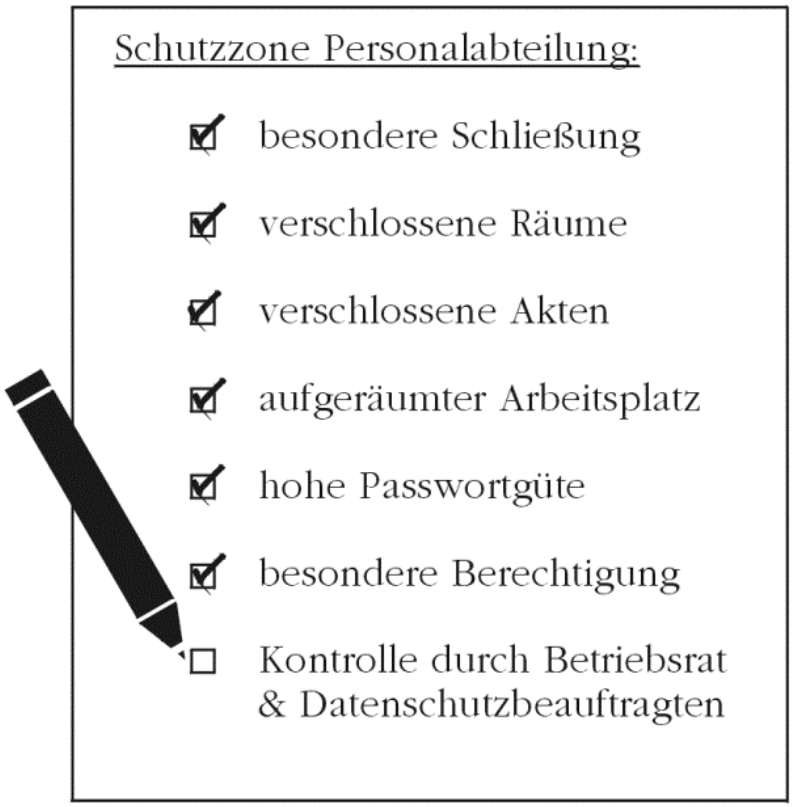
Kundendatenschutz

- Kundengewinnung
- Kundenbewerbung
- Vertragsabwicklung + Versand
- Newsletterversand
- Customer Relationship Management
- Aufbereitung & Analyse von Kundendaten (Data Warehouse)
- Betrieb eines Web-Portals
- Elektronische Kommunikation

Personalaktenführung (1)

Grundsätze:

- **Vertraulichkeit**
  → funktionstüchtiger Zugriffsschutz, da Daten nach § 3 Abs. 9 BDSG enthalten
- **Richtigkeit**
  → Personalaktendaten müssen korrekt & aktuell sein
- **Transparenz**
  → nachvollziehbare Dokumentation
- **Zulässigkeit**
  → Gestattungsgrundlage nötig



Personalaktenführung (2)

- wesentliche Vertragsbedingungen müssen auf Papier vorgehalten werden (§ 2 Abs. 1 Satz 3 NachwG), ebenso Zeugnisse (§ 630 BGB) und Ausbildungsverträge (§ 11 Abs. 1 BBiG)
- Ein Beschäftigter darf seine Personalakte vollständig einsehen (§ 83 Abs. 1 BetrVG bzw. § 68 Abs. 2 BPersVG) → Nebenakten (z.B. Akten in Zweigstelle) in Personalakte aufzuführen!
- Betroffener hat Recht auf Berichtigung unrichtiger Daten (§ 35 Abs. 1 BDSG)
- Abmahnungen sind (je nach Schwere des Vergehens) i.d.R. nach 3 Jahren aus der Personalakte zu entfernen (BAG-Urteil von 1987)
- besonderer Zugriffsschutz (z.B. verschlossener [Stahl-]Schrank) für Aufbewahrung von Personalakten erforderlich; Gesundheitsdaten (z.B. zur Schwerbehinderung) sind unter Verschluss zu halten (BAG-Urteil von 2006)

Personalaktenführung (3)

- Für Personalakten ausgeschiedener Mitarbeiter besteht keine zwingende Maximaldauer zur Aufbewahrung, empfehlenswert ist jedoch eine Aufbewahrungsfrist von mind. 10 Jahren (für Teilaspekte sind auch geringere Fristen einschlägig, doch wird eine getrennte Behandlung im Sinne von § 35 Abs. 3 Nr. 3 BDSG gemeinhin als unverhältnismäßig hoher Aufwand angesehen)
- Personalakten ausgeschiedener Mitarbeiter dürfen auch länger gespeichert werden, da der Betroffene Interesse an längerfristige Lagerung hat → hat Sperrung der Alt-Akten zur Folge
- Betroffener hat auch Einsichtsrecht in seine Personalakte nach seinem Ausscheiden bei berechtigtem Interesse – etwa zur Vorbereitung seiner Altersversorgung (BAG-Urteil von 1994)

Personalaktenführung (4)

- Zur Wahrnehmung der Führungsaufgaben ist auch Vorgesetzten eine eingeschränkte Einsicht in Personaldaten zu gewähren, soweit dies für die jeweiligen Führungsaufgaben erforderlich ist:
  - zulässig für Anwesenheitszeiten, Brutto-Gehaltsdaten & Qualifikationsdaten
  - nicht zulässig dagegen z.B. bei Angaben zu Gehaltspfändungen, familiäre Verhältnisse, Unterhaltspflichten, Netto-Gehaltsdaten & Krankenkassendaten

Personaleinstellung (1)

- Verfahren: Bewerbungsverfahren / Recruiting
- Rechtsgrundlage: § 32 Abs. 1 Satz 1 BDSG
- Nur solche Bewerbungsdaten erforderlich, die für die in Aussicht stehende Stelle benötigt werden und im sachlichen Zusammenhang mit dem angestrebten Arbeitsverhältnis stehen (BAG-Urteil von 1984)
- Vertraulichkeit der Personalakte gilt bereits für Bewerbungsdaten („culpa in contrahendo“ nach § 311 Abs. 2 BGB)
  → Für Online-Bewerbung Verschlüsselung vorsehen
- Bewerbungsdaten, die nicht mehr benötigt werden (erfolglose Bewerbung), sind unverzüglich zu löschen (nach § 35 Abs. 2 Nr. 3 BDSG)
  → Papierunterlagen an abgelehnten Bewerber zurückschicken
  → elektronische Unterlagen (Mailbewerbung/Bewerberportal) löschen
  → wegen § 15 Abs. 4 AGG (zur Abwehr der Entschädigungsklage) i.d.R. 6 Monate (berechtigtes Interesse nach § 28 Abs. 1 Nr. 2 BDSG i.V.m. § 22 AGG)

Personaleinstellung (2)

- Eingesetzte Personalberater werden i.d.R. im Rahmen einer Funktionsübertragung tätig (nur im Ausnahmefall via Auftragsdatenverarbeitung)
- Zum Fragerecht bei Vorstellungsgespräch gibt es eine umfassende Rechtsprechung
  → bei unzulässigen Fragen hat Bewerber „Recht auf Unwahrheit“
  → bei berechtigten Fragen stellt unwahre Antwort arglistige Täuschung im Sinne von § 123 BGB dar (berechtigt zur außerordentlichen Kündigung des dann auf unzutreffenden Grundlagen bestehenden Beschäftigungsverhältnisses)
  → Vorstellungsgespräch dient auch zur Erstellung eines Persönlichkeitsbildes
- Soweit Mitbestimmung zur Anwendung kommt, besteht Informationspflicht gegenüber Mitarbeitervertretung (§ 99 Abs. 1 BetrVG bzw. §§ 75 Abs. 1 Nr. 1 & 76 Abs. 1 Nr. 1 BPersVG)
- längere Aufbewahrung der Bewerbungsunterlagen möglich bis zum Antritt des positiv beschiedenen Bewerbers mit Einwilligung

Personaleinstellung (3)

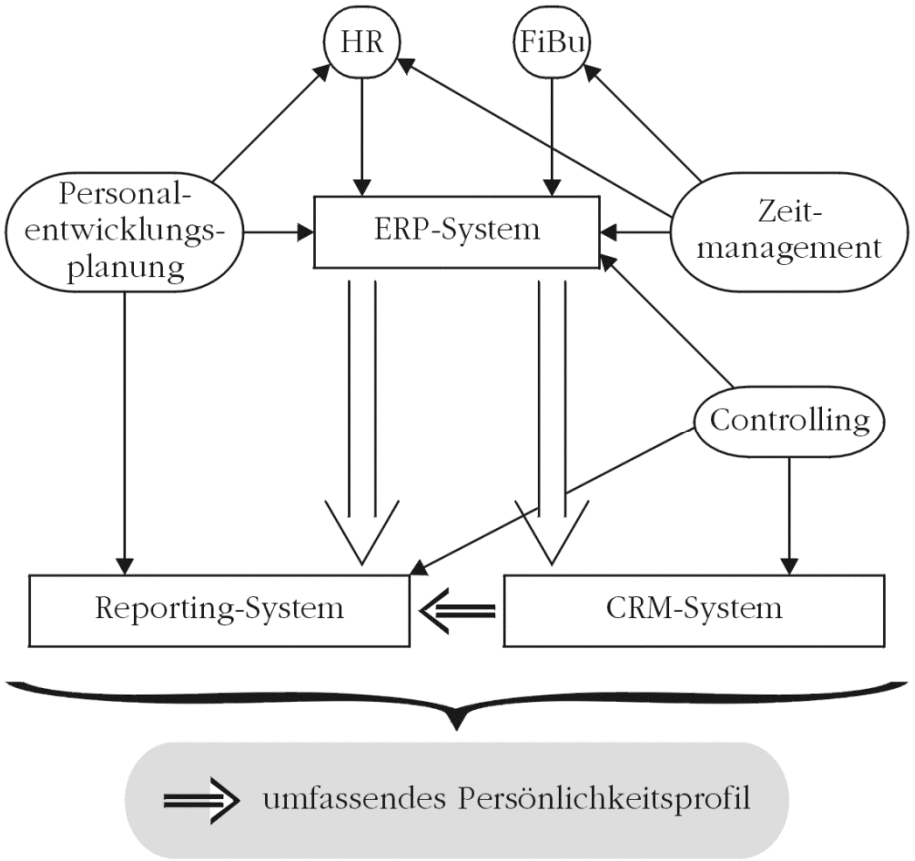
- Eigenbewertungen (Schematische Analyse der Bewerbungsunterlagen plus Mitschrieb zum Vorstellungsgespräch) sind nicht Teil der Personalakte! (→ Ablage in einer Sachakte)
- Unterlagen über Beihilfe, Lohnlisten & Arbeitsunfähigkeitsbescheinigungen ebenfalls Sachakte (letztere dennoch häufig in Personalakte vorzufinden)
- **Bewerbungsdaten erfolgreicher Bewerber sind schließlich in die Personalakte zu überführen!**
- Neue Mitarbeiter müssen i.d.R. einen Personalfragebogen ausfüllen
  → Erhebung der Stammdaten für HR-System!
  → Personalfragebogen muss sich auf erforderliche Daten beschränken (darf z.B. nur Daten über die Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft, für die Religionssteuer zu entrichten ist, erfassen)

Personaleinstellung (4)

- Bei Antritt der neuen Stelle wird oftmals eine sog. „Eintrittsuntersuchung“ durchgeführt
  → Betriebsarzt prüft arbeitsmedizinisch, ob Mitarbeiter für die vorgesehene Tätigkeit gesundheitlich in der Lage ist
  → Ergebnis im Sinne von „geeignet“, „unter bestimmten Voraussetzungen geeignet“ oder „ungeeignet“ wird dem Arbeitgeber mitgeteilt, nicht aber die Befunddaten, die zu dieser Einstufung geführt haben
  → Unterlagen zur Eintrittsuntersuchung unterliegen der ärztlichen Schweigepflicht nach § 8 Abs. 1 Satz 3 ASiG (& § 203 Abs. 1 Nr. 1 StGB)
- Teilweise setzen bestimmte Tätigkeiten besondere Nachweise voraus:
  ° polizeiliches Führungszeugnis (z.B. bei Umgang mit Bargeld)
  ° Gesundheitszeugnis (z.B. bei Umgang mit Lebensmitteln)
  ° Sicherheitsüberprüfung (z.B. bei Umgang mit geheimen Unterlagen)

Personaldatenverwaltung

- Verfahren zur Personaldatenverwaltung
  → **siehe Übungen**!
- ERP-System ist das zentrale System im Bereich des Personalwesens
  → via HR-System: Personalverwaltung
  → via Finanzbuchhaltung: Kostenstellenrechnung, Reisekosten- & Lohn-/Gehaltsabrechnung
  → via Zeitmanagement: Betriebsdatenerfassung & Arbeitszeitkontrolle



Lohn- & Gehaltsabrechnung (1)

- Aus den steuerrechtlichen Vorgaben resultiert eine umfassende **Aufbewahrungsfrist**: 10 Jahre für alle Buchungsbelege, da bilanzrelevant (§ 147 Abs. 3 AO); Geschäftsbriefe & Lohnlisten dagegen nur 6 Jahre (§ 147 Abs. 1 Nr. 2 und 5 AO); erfolgen Gehaltskürzungen auf der Grundlage fortwährender Krankschreibungen, sind diese Bescheinigungen der Krankenkassen 10 Jahre aufzubewahren
- Finanzwirksame Vorgänge (hier: Lohn- und Gehaltsabrechnung sowie Reisekostenabrechnung) müssen im Einzelnen den **Grundsätzen ordnungsgemäßer Buchführung** (§ 238 Abs. 1 HGB) entsprechen
  → keine Buchung ohne Beleg
  → vollständige Dokumentation aller Geschäftsvorfälle
  → revisionssichere (= manipulationsfeste) Archivierung
  → Revisionssicherheit muss nachweisbar sein
  → Protokollierung der Vorgänge mit Angabe der die Vorgänge bearbeitenden Beschäftigten (unter Beachtung der Datensparsamkeit)
  → regelmäßige Kontrollzyklen des internen Kontrollsystems (IKS)

Lohn- & Gehaltsabrechnung (2)

- **Archivierungspflichten** betreffen sowohl die EDV-gestützte Buchhaltung als auch die Ablage von Unterlagen / Belegen
  → Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (**GoBD**)
  → DV-System gegen Verlust zu sichern & gegen unberechtigte Eingaben und Veränderungen zu schützen
  → Nachweis via Protokollierung
  → Unveränderlichkeit via Hardware, z.B. mittels WORM-Medien
  → Unveränderlichkeit via Software, z.B. mittels Versionsionierung
- Bei Weitergabe der Verdienstabrechnung & der Meldungen zur Sozialversicherung an den Mitarbeiter ist ein geeigneter **Zugriffsschutz** umzusetzen aufgrund der darin enthaltenen besonderen Arten personenbezogener Daten (Religionszugehörigkeit, Gehaltskürzung bei lang anhaltender Krankheit, …)
  → Weitergabe mittels verschlossenem Umschlag

Mitbestimmung (1)

Mitbestimmungsrecht des Betriebsrats besteht zur:

- technischen Einrichtung, die dazu bestimmt ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen nach § 87 Abs. 1 Nr. 6 BetrVG (→ Arbeitszeitüberwachung, Videoüberwachung, …)
- betrieblichen Ordnung und zum betrieblichen Verhalten nach § 87 Abs. 1 Nr. 1 BetrVG
- Gestaltung von Personalfragebögen nach § 94 Abs. 1 BetrVG
- Regelung der betrieblichen Berufsbildung nach § 97 Abs. 2 BetrVG
- Personalauswahl und Eingruppierung oder Umgruppierung von Mitarbeitern (§ 99 Abs. 1 BetrVG) und Kündigung von Mitarbeitern (§ 102 Abs. 1 BetrVG)
- vorübergehenden Verkürzung oder Verlängerung der betriebsüblichen Arbeitszeit (§ 87 Abs. 1 Nr. 3 BetrVG) sowie zur Auswirkung dauerhaft anfallender Überstunden auf die Personalplanung (§ 92 BetrVG)

Mitbestimmung (2)

Mitbestimmungsrecht des Betriebsrats besteht zur:

- Durchführung eines betrieblichen Eingliederungsmanagements (BEM), sofern der Betroffene ausdrücklich ein BEM mittels informierter Einwilligungserklärung beantragt hat (§ 84 Abs. 2 SGB IX hinsichtlich BEM, § 87 Abs. 1 Nr. 7 BetrVG hinsichtlich Gesundheitsschutz im Betrieb und § 87 Abs. 1 Nr. 1 BetrVG hinsichtlich etwaiger Krankenrückkehrgespräche)
- Anforderung von Einzelverbindungsnachweise eingesetzter Mobiltelefone bzw. Festnetzanschlüsse. Hier muss der Teilnehmer (= verantwortliche Stelle) allen betroffenen Nutzern (= Beschäftigte, denen ein dienstliches Mobiltelefon ausgegeben bzw. der Festnetzanschluss eingerichtet wurde) über die Anforderung von Einzelverbindungsnachweise informieren und den Betriebsrat beteiligen (§ 99 Abs. 1 Satz 4 TKG)

→ **Eigene Geheimhaltungsverpflichtung (§ 79 BetrVG) neben dem Datengeheimnis (§ 5 BDSG)**

→ **Betriebsrat trotzdem auf das Datengeheimnis zu verpflichten!**

Mitbestimmung (3)

Kontrollrechte des Betriebsrats:

- Der Betriebsrat hat darüber zu wachen, dass die zu Gunsten der Arbeitnehmer geltende Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden (§ 80 Abs. 1 BetrVG)
  - → Umsetzung der Regelungen zum Arbeitnehmerdatenschutz (§ 32 BDSG)
  - → Umsetzung der Regelungen aus geltenden Betriebsvereinbarungen (datenschutzrechtlich eine vorrangige Rechtsvorschrift!)
  - → Vermeidung von Diskriminierungen (§ 75 Abs. 1 BetrVG)
- Zur Durchführung seiner Kontrollrechte muss der Arbeitgeber den Betriebsrat rechtzeitig und umfassend unterrichten (§ 80 Abs. 2 BetrVG) und daher auf Verlangen die erforderlichen Unterlagen zur Verfügung stellen
  - → Einsicht in Lohnlisten (aber nicht ins HR-System!)
  - → Übersichten zur Arbeitszeitentwicklung
  - → Berichte zu durchgeführten Datenschutzkontrollen

Mitbestimmung (4)

Kontrollrechte des Betriebsrats:

- Zudem hat der Arbeitgeber den Betriebsrat rechtzeitig unter Vorlage der erforderlichen Unterlagen über seine Planungen zu unterrichten (§ 90 Abs. 1 BetrVG) zu baulichen Maßnahmen, technischen Anlagen, Arbeitsverfahren und –abläufen (betrifft z.T. auch Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben) sowie zu Arbeitsplätzen
- Der Betriebsrat kann zur Durchführung seiner Kontrollrechte Sachverständige (wie z.B. den Datenschutzbeauftragten) hinzuziehen