

# Workshop 2

## Datenschutz und SAP

Workshop 2a: Lorenz Hinrichs, TBS Niedersachsen gGmbH  
Jochen Brandt, Brandtschutz Hamburg

Workshop 2b: Horst Kübeck, g·ibs Berlin mbH  
Friedhelm Michalke, TIB Hamburg

## **Datenschutz im Sinne des BDSG bedeutet Persönlichkeitsschutz**

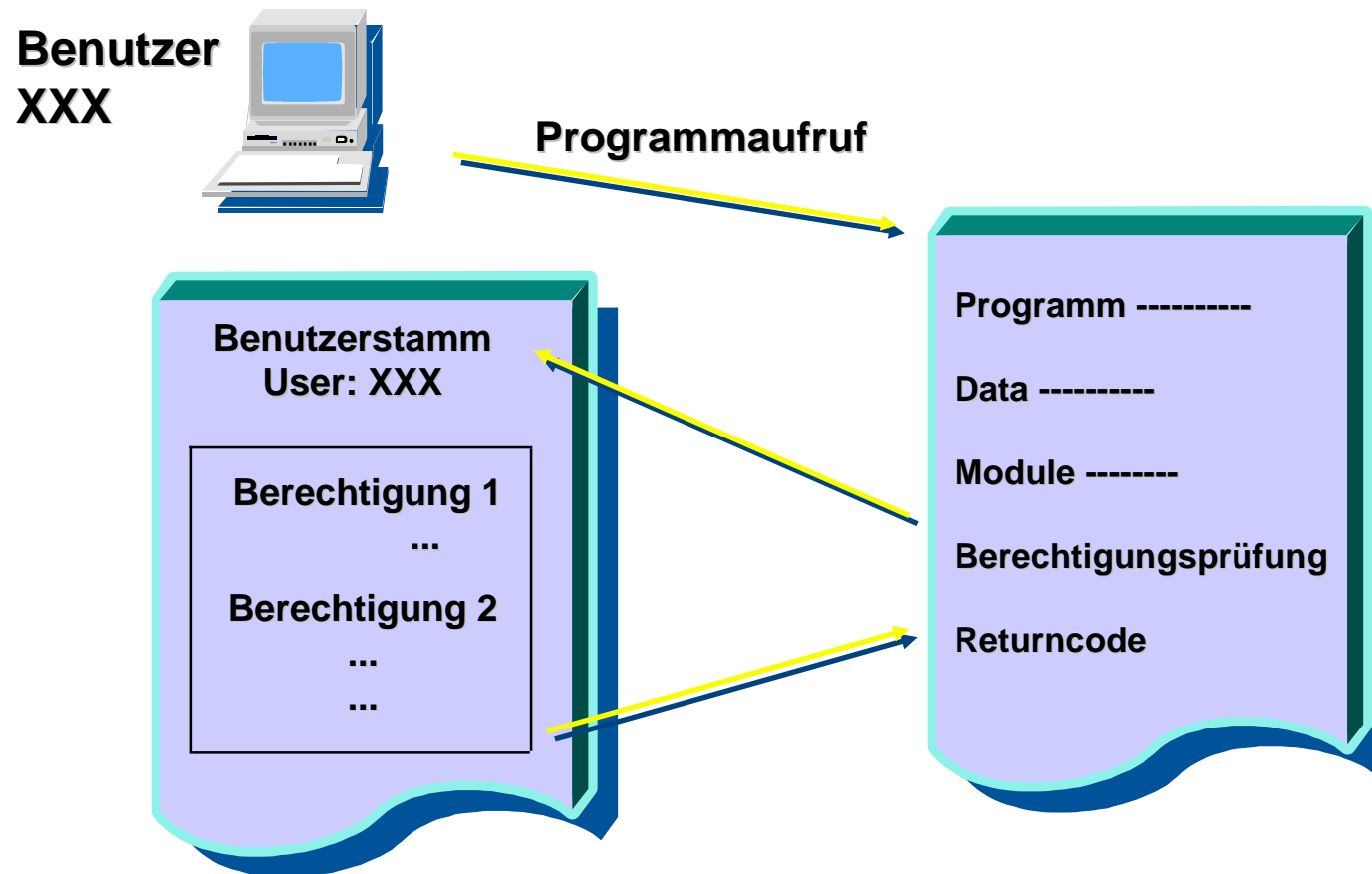
Bei der Datenverarbeitung mit SAP  
ist das BDSG einzuhalten:

Welche personenbezogenen Daten  
werden warum vom Betrieb  
gespeichert?

Wer darf warum auf diese Daten  
zugreifen oder sie ändern?



## Berechtigungsprüfung in SAP beim Programmaufruf



## **SAP kennt keine Regeln, welche Personendaten angelegt werden dürfen**

Das Einhalten der Regelungen des  
BDSG ist dem Kunden überlassen  
Belegschaftsvertretungen müssen  
hier Einfluss nehmen!

SAP ermöglicht nur einen gewissen  
technischen Schutz vor unbefugten  
Zugriffen und deren Überprüfung

## **SAP legt nicht automatisch die geforderten Verzeichnisse an**

Das BDSG verlangt in §4e,g zwingend die Erstellung von Verzeichnissen.

Diese geben auch für den BR / PR Auskunft über die Verarbeitung von Belegschaftsdaten.

Zu SAP müssen diese ohne SAP-Hilfen vom Betrieb selbst erstellt werden.

## Verfahrensverzeichnis nach §4e BDSG

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der Kategorien der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

**Unterschriften Geschäftsführung, Datenschutzbeauftragter, Betriebsrat?**

# Datenschutz, insbesondere grenzüberschreitender Datentransfer

# Datenverarbeitung im Auftrag

# Datenverarbeitung im Auftrag

Vorgaben durch § 11 BDSG:

- Auftraggeber ist für die Einhaltung des BDSG und anderer Rechtsvorschriften für den Datenschutz verantwortlich
- Recht auf Schadenersatz ist gegenüber dem Auftraggeber geltend zu machen
- Sorgfältige Auswahl des Auftragnehmers unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen

# Datenverarbeitung im Auftrag

Vorgaben durch § 11 BDSG:

- Auftragserteilung hat schriftlich zu erfolgen
  - Festlegung der technischen und organisatorischen Maßnahmen
  - Festlegung von eventuellen Subunternehmern/-auftragnehmern
- Auftraggeber hat sich von der Einhaltung der techn. und organ. Maßnahmen beim Auftragnehmer zu überzeugen
- Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten darf sich nur im Rahmen der Auftragserteilung bewegen
- Auftragnehmer hat Auftraggeber auf Verstöße gegen das BDSG hinzuweisen

# Datenverarbeitung im Auftrag

## Arten von Auftragsdatenverarbeitung:

- Lohn-/Gehaltsabrechnung
- Datenerfassung
- Befragungen/Umfragen
- Archivierungen
- Löschung von Datenträgern
- postalische und/oder elektronische Mailings
- Administration und Wartung der IT
- Programmierung und Customizing

# Datenverarbeitung im Auftrag

Spezialfall: Datenverarbeitung im Auftrag innerhalb eines Konzerns.

- Kein Konzerprivileg im Datenschutz
- Die Daten der einzelnen Konzernteile sind strikt zu trennen.
- Eine gemeinsame DV würde das Prinzip des § 11 BDSG verletzen.
- Die gemeinsame Verarbeitung von Daten muss auf einer anderen Rechtsgrundlage beruhen.

# Datenübermittlung ins Ausland

## § 4b BDSG: Übermittlung personenbezogener Daten ins Ausland

- Innerhalb der Mitgliedstaaten der EU sieht das BDSG „freien Datenverkehr“ vor
- Folge ist, dass die Bewertung des Datenverkehrs von Hannover nach Berlin identisch zu werten ist wie der von Hannover nach Paris
- Datentransfer in Drittländer, die sich außerhalb der EU befinden, ist nur dann zulässig, wenn das Drittland ein angemessenes Datenschutzniveau gewährleistet

## § 4b BDSG: Übermittlung personenbezogener Daten ins Ausland

- **Angemessenheit des Datenschutzniveaus** wird unter Berücksichtigung der Umstände beurteilt
- Dazu herangezogen werden u.a.:
  - Art der Daten
  - Dauer der geplanten Verarbeitung
  - Herkunfts- und Empfängerland
  - Für den Empfänger geltende Rechtsnormen und Sicherheitsmaßnahmen
- Die Verantwortung für die Übermittlung trägt die übermittelnde Stelle
- Der Empfänger ist darauf hinzuweisen, dass Daten Zweckgebunden zu verarbeiten sind

# Anwendungsbereich

- Grundsätzlich gilt der freie Datenverkehr innerhalb der EU/EWR-Staaten
- Bei Übertragung in Drittstaaten ist darauf zu achten, ob eine positive Feststellung bzgl. des Schutzniveaus des Empfängerlandes vorliegt
  - Wenn negativ: kommt einer der Ausnahmetatbestände nach § 4c in Betracht
    - Ebenfalls negativ: Feststellung, ob beim Empfänger im Drittland ein angemessenes Schutzniveau vorliegt
- **PROBLEMATISCH** ist dabei **IMMER** die Übertragung von Mitarbeiterdaten

## § 4c BDSG: Ausnahmen (1)

### Safe-Harbour-Principles

Hierbei handelt es sich um Datenschutzgrundsätze, denen sich US-Unternehmen freiwillig unterwerfen können, wenn sie Daten aus der EU erhalten.

Bei den angeschlossenen Unternehmen wird das Vorliegen eines angemessenen Schutzniveaus vorausgesetzt.

Die Prinzipien des Safe-Harbour gleichen denen der EU-Datenschutz-Richtlinie. Die angeschlossenen Unternehmen werden regelmäßig dahingehend überprüft, ob sie das Schutzniveau einhalten und gewährleisten.

## § 4c BDSG: Ausnahmen (2)

### EU-Standardvertragsklauseln

Da die Feststellung über das Herstellen eines angemessenen Datenschutzniveaus in einem Drittland sich schwer verwirklichen lassen kann, hat die EU-Kommission **Standardvertragsklauseln** verabschiedet.

Eine weitere Prüfung durch die Aufsichtsbehörde kann entfallen; Vertrag ist jedoch vorzulegen (§ 38 BDSG)

# Inhalt der EU-Klausel

- **Normativer Teil**
  - Begriffsbestimmung
  - Pflichten der beteiligten Parteien
  - Haftung; Rechte Dritter
  - Schlichtungsverfahren und Gerichtsstand
  - Zusammenarbeit mit Kontrollstellen
  - Beendigung des Vertrages
- **Anhänge**
  - Festlegungen (etwa Datenimporteur und Datenexporteur)
  - Regelungen zum technischen und organisatorischen Datenschutz)

## § 4c BDSG: Ausnahmen (3)

### Code of Conduct

Hierbei handelt es sich um verbindliche Unternehmensregelungen, die innerhalb eines Konzerns abgeschlossen werden können. Zwei Standardwerke sind durch den „Düsseldorfer Kreis“ bereits abgestimmt worden.

Gegenstand sind auch hier einzelne Übermittlungen bzw. bestimmte Arten von Übermittlungen, die international im Konzern mit Schutzgarantien für die Beteiligten zu vereinbaren sind.

[www.datenschutz-berlin.de/jahresbe/02/anl/anlagenband2002.pdf](http://www.datenschutz-berlin.de/jahresbe/02/anl/anlagenband2002.pdf)

## Aber ...

... der Rückgriff auf  
Standardvertragsklauseln führt nicht  
dazu, dass das BetrVG außer Kraft  
gesetzt wird.

# Zulässigkeitskriterien

- Nach BDSG zwei Schritte:
  - Übermittlung muss zulässig sein
  - Voraussetzungen einer Übermittlung ins Ausland müssen gegeben sein
- Sonderfall Betriebsvereinbarung
  - Gilt nicht für das Ausland; kann jedoch den „Fluss“ der Mitarbeiterdaten reglementieren.
- Genehmigung
  - Gemäß § 4c Abs. 2 BDSG kann die Aufsichtsbehörde Datentransfer genehmigen. Voraussetzung ist auch hier das Vorliegen von Schutzgarantien.

# Umgang mit Arbeitnehmerdaten - Beispiele -

# Die Beispiele

## National

1. Zentralisierung von Aufgaben im deutschen Konzern
2. Auslagerung von Verwaltungsaufgaben an ein externes Unternehmen

## International

3. Weltweiter Datenaustausch innerhalb eines Konzerns
4. Leistungskontrolle in einem Drittland
5. Buchhaltung in Indien
6. Vertrieb in Prag
7. Skill-Management in der Karibik

## 1. Zentralisierung von Aufgaben im deutschen Konzern

- Aufgaben wie etwa Gehaltsbuchhaltung sind/werden in vielen deutschen Konzernunternehmen zentralisiert
- Teilweise gibt es hierfür keine expliziten Datenschutzregelungen
- Entsprechendes gilt für zentrale und unternehmensübergreifende Skill-Management- und Wissensmanagement-Systeme

## 2. Auslagerung von Verwaltungsaufgaben an ein externes Unternehmen

- Übertragungen von Leistungen an externe Dienstleister sind in Deutschland häufig
- Beispiele:
  - Reisekostenabrechnung
  - IT-Management
  - Buchhaltung
  - ...

### 3. Weltweiter Datenaustausch innerhalb eines Konzerns

Ein US-Konzern, der Dienstleistungen im IT-Bereich anbietet, will alle weltweit operierenden Konzerntöchter per Vertrag in die Lage versetzen, vorhandene personenbezogene Daten weltweit wechselseitig zu verarbeiten.

## 4. Leistungskontrolle in einem Drittland

- Ein deutscher Konzern wickelt DV-Prozesse mit SAP über einen zentralen Server in den USA ab. Betrieben wird dieser von einer dort ansässigen Tochter
- Demnächst sollen Auswertungen zu den individuellen Leistungen der Mitarbeiter von der US-Tochter durchgeführt werden
- Im Konzern werden keine nennenswerten datenschutzrechtlichen Probleme gesehen, weil eine Reihe von deutschen Mitarbeitern der Verarbeitung zugestimmt haben

## 5. Buchhaltung in Indien

- Eine deutsche Tochter eines ausländischen Unternehmens wickelt die gesamte Buchhaltung in Indien über ein indisches Unternehmen ab
- Das indische Unternehmen garantiert den Datenschutz, spezielle Regelungen sind nicht fixiert worden
- Weder die Kunden in Deutschland noch die betroffenen Arbeitnehmer sind über den Datentransfer informiert worden

## 6. Vertrieb in Prag vs. Goa

- Ein deutscher Konzern strukturiert derzeit seine weltweiten Aktivitäten neu. In diesem Rahmen werden beispielsweise Kundenservice, Vertrieb sowie die Buchhaltung ausgelagert (Offshoring)
- Soweit direkte Kontakte in deutscher Sprache erforderlich sind, erfolgt eine Verlagerung nach Prag
- Soweit keine direkten Kontakte nach Deutschland erforderlich sind oder wenn diese in englischer Sprache erfolgen können, erfolgt die Verlagerung nach Indien
- Im Bereich des Datenschutzes werden keine Probleme gesehen. Der US-Anbieter des Offshoring versichert, dass alle nationalen Vorgaben berücksichtigt werden

## 7. Skill-Management in der Karibik

- Das zentrale Skill-Management-System in einem Konzern wird nunmehr von einer Tochter durchgeführt, angesiedelt auf einer Karibik-Insel
- Manager wie Mitarbeiter sollen in den nächsten Monaten umfassende Profildaten in ein elektronisches System eingeben
- Das System soll u.a. die berufliche Weiterentwicklung der Arbeitnehmer fördern
- Datenschutzrechtliche Probleme sind bisher im Management der deutschen Konzerntochter nicht gesehen bzw. diskutiert worden

## Anforderungen an ein Datenschutzmanagement

Die Anforderung an ein Datenschutzmanagement können unter Umständen sehr hoch sein. Sollten einzelne Anforderungen nicht eingehalten werden kann dies Konsequenzen für die gesamte Datenverarbeitung haben.

So verurteilte das Landgericht Gießen eine Behörde zur Löschung einer kompletten Skilldatenbank, da ein fehlendes Verzeichnisse und eine nicht durchgeführte Vorabkontrolle dazu führe, dass die personenbezogenen Daten in diesem System nicht sicher seien.

## Gemeinsames Seminarprogramm

der Unternehmensberatungen für  
Arbeitnehmervertretungen



Berlin



Berlin



Hannover



Hamburg

**Wir beraten Betriebs- und Personalräte**