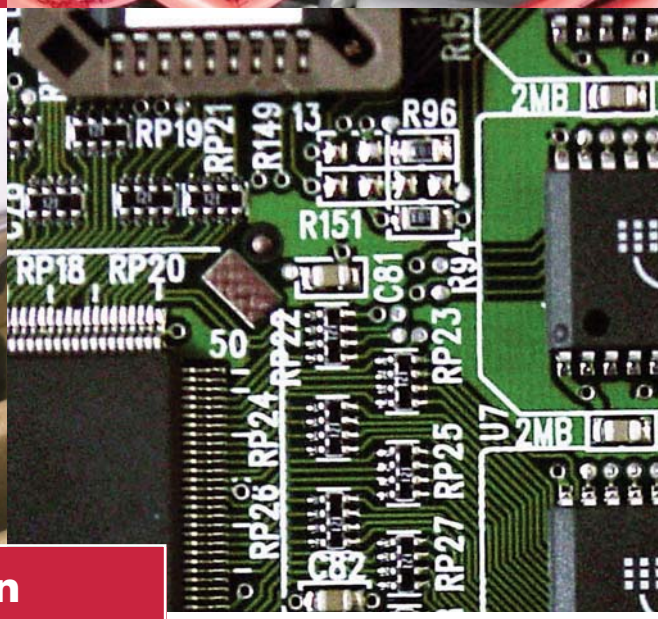
# Fahren Sie nach Indien!

# Ihre Daten sind schon dort!






**Informationen und Handlungshilfen**
zum grenzüberschreitenden Datentransfer

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Die weibliche Endung wird in der Broschüre dann verwendet, wenn tatsächliche Personen gemeint sind, wenn allgemein von Institutionen, Organisationen oder juristischen Personen(-gruppen) die Rede ist, wird - wie in der einschlägigen Texten allgemein üblich - nur die männliche Form benutzt (z.B. Auftraggeber, Empfänger, Dienstleister, ….).

**Impressum:**

Herausgeber: Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier, 1034 Wien, Alfred-Dallinger-Platz 1

AutorInnen: GPA-DJP Arbeit und Technik, IG work@IT

Layout: GPA-DJP Marketing, Eveline Pelzer

Fotos: Bilderbox

Wien, Dezember 2007

# Vorwort

**Liebe Kollegin, lieber Kollege,**

Lohnverrechnung outgesourct nach Indien, Personalbemessung zentralisiert in der holländischen Konzernzentrale, allgemeines KundenInnenservice im us-amerikanischen Schwester-Konzern. Wer hat in letzter Zeit nicht von solchen Vorgängen in weltweit agierenden Unternehmen gehört?

Die Organisationsstruktur von Konzernen wandelt sich immer stärker in Richtung so genannter „Matrixstrukturen". Das bedeutet Vorgesetzte und MitarbeiterInnen sind weltweit verstreut. Um dennoch miteinander kommunizieren zu können, braucht es - so die Konzernleitungen - zentralisierte und vereinheitlichte Personalverwaltungssysteme. Innerhalb solch komplexer Strukturen und konzentrierter Personalsysteme findet sich der/die Einzelne immer weniger zurecht.

Zugleich zu den versprengten Organisationsstrukturen sollen aber die Daten der einzelnen MitarbeiterInnen bis hinauf in die höchsten Ebenen der Konzernleitung einsehbar sein und von dort auch gesteuert werden können. Sprich: Das Human-Ressource-Management in den USA, fünf Ebenen über der nationalen Abteilungsleitung, entscheidet, wer versetzt wird, wer eine Leistungsprämie erhält, wer welche interne Weiterbildung erhält oder wer das Unternehmen verlassen muss.

In der täglichen Beratung sind wir in der GPA-djp immer häufiger mit dem komplexen Thema Datenschutz konfrontiert. Ein geringer Wissensstand zu dem Thema bei vielen ArbeitnehmerInnen und BetriebsrätInnen, und eine geringen Sensibilität auf allen Ebenen der Unternehmen haben uns dazu veranlasst, eine Broschüre zum Datenschutz für MitarbeiterInnen-Daten zu schreiben.

Nicht zuletzt haben das Engagement des Beirats für Arbeit & Technik sowie der FunktionärInnen der Interessengemeinschaft work@IT wesentlich dazu beigetragen, dass diese Broschüre entstehen konnte.

Entstanden ist ein umfassendes Werk, das sich mit Datenschutz aus allen Perspektiven beschäftigt. Es werden sowohl die rechtlichen als auch die technischen Aspekte des Datenschutzes beleuchtet. Kernstück der Broschüre ist der strategische Teil. Darin werden sowohl Argumente zur Überzeugungsarbeit und Sensibilisierung vorgestellt, als auch praktische Handlungshilfen, wie man den Datenschutz innerbetrieblich verbessern kann.

Auch das GPA-djp-Bundesforum hat schon im Jahr 2006 den Schutz von MitarbeiterInnendaten zum Thema gemacht und eine gesetzliche Verpflichtung gefordert zur Einrichtung unabhängiger betrieblicher Datenschutzbeauftragter. Diese Forderung möchten wir in dieser Broschüre erneuern und gleichzeitig genauer darstellen, welche Rechte und Pflichten die mit dem Datenschutz beauftragten Personen im Betrieb haben sollten.

**Viel Erfolg bei der Arbeit für einen besseren Schutz der Daten eurer MitarbeiterInnen!**

**Wolfgang Katzian**
Vorsitzender

# Inhalt

# GUTE ARBEIT

Arbeit ist eines der bedeutendsten Räder im Getriebe der Gesellschaft und hält das tägliche Leben in allen uns bekannten Formen am Laufen. Deshalb bestimmt die Art und Weise, wie wir arbeiten auch wesentlich über unsere allgemeine Zufriedenheit und Lebensqualität mit. Doch stetig wachsende Produktivitäts- und Gewinnerwartungen steigern die Anforderungen an ArbeitnehmerInnen und erhöhen den Druck am Arbeitsplatz. BetriebsrätInnen und Gewerkschaften sind daher stets bemüht, arbeitsrechtliche Standards zu bewahren und mehr als nur menschenwürdige Arbeitsbedingungen zu sichern, damit die steigende Produktivität auch denjenigen zugute kommt, die diese erwirtschaften – den Arbeitnehmerinnen und Arbeitnehmern. Diese Aufgabe wird gerade in wirtschaftlich schlechten Zeiten zu einer immer schwierigeren Herausforderung.

**Arbeit um jeden Preis?** Die schlechte Arbeitsmarktsituation und die Notwendigkeit, um Arbeitsplätze zu kämpfen, wird oft als Rechtfertigung benutzt, um Qualitätsstandards bei den Arbeitsbedingungen auszuhöhlen bzw. eine Weiterentwicklung zu verhindern. **Beschäftigungssicherung geht Hand in Hand mit dem Erhalt und der Verbesserung von Arbeit.** In dieser Frage kann es **nicht** heißen: **„entweder – oder". Wir fordern beides!**

**Die Beschäftigten haben es sich verdient!**
**Wir wollen GUTE ARBEIT, um gute Arbeit leisten zu können!**

Wir knüpfen damit an bisherige Bemühungen sowohl unserer eigenen gewerkschaftlichen Arbeit als auch an internationale Erfahrungen an. Es ist notwendig für GUTE ARBEIT einzutreten und es lohnt sich auch. **Dabei geht es in erster Linie darum, die Stimmen derer zu hören, die ExpertInnen in der Beurteilung ihres Arbeitsumfeldes sind: die Beschäftigten.** Die GPA-djp stellt Informationen zur Erfassung des Arbeitsklimas im Betrieb bereit und gibt Handlungshilfen für die Gestaltung von Arbeitsplätzen. In der Reihe GUTE ARBEIT berücksichtigen wir jene Bereiche, die Arbeitsprozesse wesentlich bestimmen:

- Beschäftigung und Einkommen
- Arbeitsorganisation
- Mitbestimmung im Betrieb
- Gesundheit und Sicherheit am Arbeitsplatz
- Aus- und Weiterbildung
- Vielfalt und Chancengleichheit

Mehr Informationen zum Thema GUTE ARBEIT unter **www.gpa-djp.at/gutearbeit**

# 1) Einleitung

**Daten in einer vernetzten Wirtschaft**

Im Zeitalter einer global vernetzten Wirtschaft sind global versprengte Konzernstrukturen immer häufiger. Es besteht gerade in großen Unternehmen ein Interesse der Konzernleitung, grenzüberschreitend auf die Daten aller MitarbeiterInnen zugreifen zu können und die Daten dann auch weiterverarbeiten zu können. Den Ideen zum Datentransfer sind dabei keine Grenzen gesetzt - Personaldatenverarbeitung bei der Konzernmutter in den USA, Personalbemessung über die Konzernzentrale in Holland, Lohnverrechnung in Indien, etc. Die Auswirkungen von konzernweiten Rankings gehen in Richtung „gläserne Belegschaft" und sind in ihrer gesamten Tragweite für den Schutz persönlicher Daten noch nicht abzusehen. Datenschutzprobleme treten auch deshalb auf, weil der Umgang mit dem Schutz persönlicher Daten und der Privatsphäre national stark variiert.

Outsourcing, internationales Ranking, Umstrukturierung oder Zentralisierung sind meist der Hintergrund vor dem sich internationaler Datentransfer von Personaldaten abspielt. Doch es ist gar nicht nötig, über die Landesgrenzen zu gehen. Auch innerhalb Österreichs kann es zu Datenschutzproblemen kommen, wenn persönliche Daten an andere Unternehmen weiter gegeben werden. Die Übermittlung personenbezogener Daten stellt oft einen enormen Eingriff in die Persönlichkeitsrechte der ArbeitnehmerInnen dar.

**Daten in Unternehmen**

Die Reichweite der Datenerfassung in einem Unternehmen ist den MitarbeiterInnen oft (noch) nicht bewusst. Zahlreiche IT-Systeme kreieren persönliche Daten:

- Zeiterfassungssysteme,
- Personalverrechnungssysteme,
- Zutrittsbeschränkungen,
- Protokollierung von Internet-Aktivitäten,
- Systeme die MitarbeiterInnengespräche und Zielvereinbarungen speichern,
- Datenbanken über Weiterbildungs(miss-)erfolge,
- Drucker, Laptops können zur MitarbeiterInnendatenerfassung herangezogen werden.

All diese Daten können gespeichert, verarbeitet, weitergegeben, verknüpft u.s.w. werden. Die Möglichkeiten zur Auswertung und zum Informationsgewinn sind unbegrenzt - die Frage ist, ob sie sinnvoll sind und ob sie mit dem Datenschutz konform sind.

**Rechtslage**

Um die MitarbeiterInnen-Daten besser vor Missbrauch zu schützen, bieten zwei Gesetzestexte die rechtliche Grundlage; das **Arbeitsverfassungsgesetz** mit seinen Mitbestimmungspflichten für den Betriebsrat und das **Datenschutzgesetz** mit seinen Melde- und Genehmigungspflichten zum Datentransfer. Beide sind als gleichwertige Rechtslagen zu sehen; Eines kann das Andere nicht ersetzen. Daher sind auch beide Gesetze in dieser Broschüre umfassend dargestellt.

**Österreich im EU-Vergleich**

10 % der europäischen Firmen schickt personenbezogene Daten in Drittländer; in Österreich sind es 11 %. 21 % der Daten, die von europäischen Firmen in Drittstaaten transferiert werden sind Personaldaten - so das Eurobarometer 2003.

Das Eurobarometer wurde durchgeführt im Auftrag der EU von Gallup Europe und befragte die unternehmensinternen Verantwortlichen für Datensicherheit. Es stellte fest, dass in Österreich das Vertrauen in den Datenschutz höher ist als in anderen EU-Staaten. Die nationale Gesetzgebung wird als ausreichend empfunden und die Besorgnis über Datenmissbrauch hält sich in Grenzen. 42 % führen allerdings eine **ungenügende Einhaltung des Datenschutzrechts** darauf zurück, dass die nationale Kontrollbehörde kaum aktiv wird und somit das Risiko bestraft zu werden, eher gering ist. EU-weit beträgt dieser Prozentsatz nur 28%. Außerdem unterscheidet sich Österreich in der Umfrage auffällig von anderen EU-Staaten in punkto **Verbesserungswünsche**. Hierzulande hätte man gerne einheitlichere Regelungen zu Sicherheitsmaßnahmen (52 % in Österreich, 33 % in der EU) und einheitlichere Informationspflichten für die Betroffenen (44 % in Österreich, 35 % in der EU).

# 2) **Worum geht's?** Begriffserklärungen zum Datenschutz

**Datensorten**

Es gibt eine ganze Menge an Daten, die Auskunft über eine Person geben: Name, Geburtsdatum, Familienstand, Anzahl der Kinder, Haar- und Augenfarbe, Schuhgröße und Adresse zählen ebenso dazu wie Religionsbekenntnis, Gehalt, Arbeitszeit, Zielvereinbarungen mit dem/der Vorgesetzten, etc.. ArbeitgeberInnen speichern viele dieser Daten systematisch und elektronisch. Welche Daten auf welche Weise verwendet werden dürfen, ist auf Basis der EU-Rahmenrichtlinie in Österreich im Datenschutzgesetz (DSG) gesetzlich geregelt.

## 2.1 Was für Daten gibt es überhaupt?

Das DSG unterscheidet vier verschiedene Arten von Daten:

- „indirekt personenbezogene Daten"
- „personenbezogene Daten"
- „besonders schutzwürdige Daten" und
- „sensible" Daten (§4 Z1 und 2 DSG).

### 2.1.1 indirekt personenbezogene Daten

**indirekt personenbezogene Daten**

Indirekt personenbezogene Daten können nicht einer bestimmten Person zugeordnet werden - zumindest nicht auf legalem Weg. Aber bestimmte Stellen (z.B. Behörden) können indirekt personenbezogene Daten zu direkt personenbezogenen Daten machen (z.B. das Kfz-Kennzeichnen, kann von der Verkehrsbehörde direkt einer Person zugeordnet werden, von einem „Park-Sheriff" aber nicht).

**österreichischer Sonderweg**

Indirekt personenbezogene Daten sind eine Sonderbestimmung für Österreich. Die EU und die meisten ihrer Mitgliedsländer kennt diese Art von Daten nicht. Diese Datenart wird in der EU nicht extra ausgewiesen sondern fällt nach EU-Definition unter „personenbezogene Daten".

**anonyme Daten**

Erst wenn die Identität einer Person überhaupt nicht mehr feststellbar ist, spricht man von anonymen Daten.

### 2.1.2 personenbezogene Daten

**personenbezogene Daten**

„Personenbezogene Daten" sind - wie der Name schon sagt - Daten, die direkt auf eine Person bezogen werden können, wobei sowohl reale Personen als auch juristische Personen (also z.B. Firmen) damit gemeint sind. Es handelt sich dabei um sämtliche Informationen, die mit einer Person oder einem Unternehmen direkt in Verbindung gebracht werden können:

- ☐ (Firmen-)Name
- ☐ Adresse
- ☐ Umsatz des Unternehmens
- ☐ Geburtsdatum des/der Mitarbeiters/in
- ☐ Sozialversicherungsnummer des/der Mitarbeiters/in
- ☐ Personalnummer des/der Mitarbeiters/in
- ☐ Qualifikation des/der Mitarbeiters/in
- ☐ Leistungsbeurteilung des/der Mitarbeiters/in
- ☐ Biometrische Daten (Fingerabdruck, Irisscan, etc.)
- ☐ Standortdaten (z.B.: Mobiltelefonie, GPS, etc.)
- ☐ Werturteile (z.B.: „zahlt schlecht").

Wo all diese Daten gespeichert werden, ist für den Datenschutz irrelevant. Egal auf welchen Bild- und Tonträgern, ob auf einer Festplatte, Diskette, CD-Rom oder Papier; die eindeutige Feststellbarkeit der Identität des/der Betroffenen ist ausschlaggebend dafür, dass diese Daten vor unerlaubtem Zugriff geschützt werden müssen.

**Ort der Datenspeicherung**

Die Identität der Person kann entweder „bestimmt" oder „bestimmbar" sein. Beide Fälle sind datenschutzrechtlich geregelt. „Bestimmt" bedeutet, dass die Daten dem/der Betroffenen zugeordnet sind, z.B.: Karl Pick, geb. 13.01.1900. „Bestimmbar" bedeutet, dass es sich um verschlüsselte Daten handelt, aber ein Schlüssel vorhanden ist mit dem die Daten jederzeit entschlüsselt werden können.

**bestimmbare Identität**

## 2.1.3 sensible Daten

**sensible Daten**

Bei sensiblen Daten handelt es sich ausschließlich um Daten von Menschen, nicht um Unternehmensdaten. Es ist generell verboten, diese Daten zu verwenden. Sie dürfen nur unter ganz bestimmten Voraussetzungen verwendet werden (§ 9 DSG).

**Folgende Daten sind sensible Daten:**

- ☐ rassische und ethische Zugehörigkeit
- ☐ religiöse und philosophische Überzeugungen
- ☐ politische Meinung, Gewerkschaftszugehörigkeit
- ☐ persönliche Sexualität
- ☐ Gesundheit

## 2.1.4 besonders schutzwürdige Daten

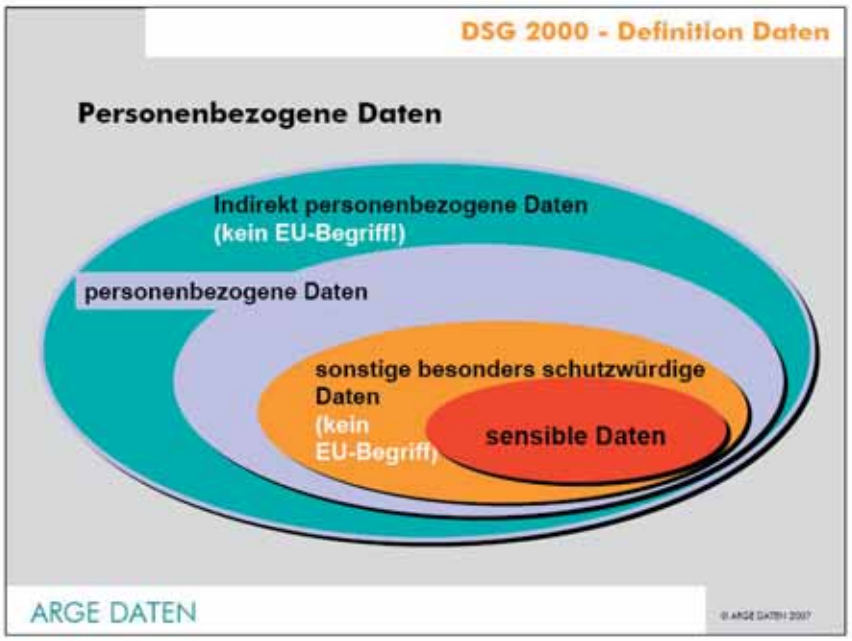
**besonders schutzwürdige Daten**

Das österreichische DSG kennt zusätzlich zu sensiblen Daten auch „besonders schutzwürdige Daten". Damit sind folgende Bereiche gemeint:

- strafrechtliche Daten
- Daten zur Beurteilung der Kreditwürdigkeit einer Person
- Daten aus einem Informationsverbundsystem (zum Informationsverbundsystem siehe Kapitel 2.4.5).

**österreichischer Sonderweg**

Diese österreichische Lösung kennt die EU nicht. In der EU-Richtlinie sind diese Daten unter den sensiblen Daten subsumiert.



## 2.2 Was ist eine Datenanwendung?

**Datenanwendung**

Zur Datenanwendung ist einem vielleicht noch der früher verwendete Begriff „Datenverarbeitung" geläufig. Man versteht darunter alle logisch miteinander verbundenen Schritte mit demselben Ziel, soweit diese Verarbeitungsschritte zumindest teilweise automationsunterstützt erfolgen. Datenanwendungen sind also beispielsweise die Personalverwaltung, die Datenbank zur Kundenbetreuung, die Auftragsdatenbanken, der automationsunterstützte Einkauf und die Lagerverwaltung aber auch das interne Telefonverzeichnis, oder die internen Leistungsbeurteilungssysteme - soweit sie automationsunterstützt und systematisch erfasst werden.

## 2.3 Was ist eine Datenverwendung?

**Datenverwendung**

Die Datenverwendung ist die Tätigkeit mit der Datenanwendungen vollzogen werden. Verb ist die Datenverwendung, Objekt ist die Datenanwendung. Bleibt man bei diesem Bild des Satzbaus, wären dann die Subjekte in dem Satz Empfänger, Betroffene, Auftraggeber, Dienstleister, etc. (siehe Kapitel 2.4).

Das österreichische DSG kennt zwei große Anwendungsbereiche für Daten:
**Datenverwendung und Datenübermittlung**

„Datenverwendung" ist der Sammelbegriff für jegliche Tätigkeit in Zusammenhang mit Daten von der Erfassung über die Verarbeitung bis hin zum Übermitteln (§ 4 Z 8-11 DSG). Es fällt darunter das:

- ☐ Ermitteln, Erfassen, Erheben
- ☐ Speichern, Aufbewahren
- ☐ Ordnen, Vergleichen
- ☐ Ändern
- ☐ Verknüpfen
- ☐ Vervielfältigen
- ☐ Abfragen, Ausgeben, Benützen
- ☐ Sperren, Löschen,Vernichten.

**Überlassung und Übermittlung**

Für den Datentransfer relevant sind die Begriffe **„Überlassung"** und **„Übermittlung"** von Daten.

- ☐ Überlassen ist die Weitergabe von Daten vom Auftraggeber an einen Dienstleister.
- ☐ Übermitteln ist sowohl
  - das Veröffentlichen von Daten,
  - die Verwendung von Daten für ein anderes Gebiet, einen anderen Zweck als in Auftrag gegeben wurde als auch
  - die Weitergabe von Daten. Nicht gemeint ist damit die Weitergabe von Daten an betroffene Personen oder den/die AuftraggeberIn oder eineN DienstleisterIn, auch nicht gemeint ist damit die Weitergabe von Daten zum selben Zweck innerhalb des selben Geschäftsbereiches.

## 2.4 Wer sind die handelnden Personen?

### 2.4.1 BetroffeneR

**Betroffene**

Der/die Betroffene ist jene Person oder jenes Unternehmen, dessen Daten verwendet werden. In der Sprache der JuristInnen gesprochen heißt das: „der/die Betroffene ist jede vom Auftraggeber verschiedene natürliche oder juristische Person, deren Daten verwendet werden" (§ 4 Z 3 DSG).

### 2.4.2 Auftraggeber

**Auftraggeber**

Auftraggeber sind diejenigen, die Daten für einen bestimmten Zweck bearbeiten, verwenden, weiterleiten, etc. Ein Unternehmen beispielsweise, das die Daten seiner MitarbeiterInnen für die Buchhaltung zur Lohnverrechnung verarbeitet, ist Auftraggeber. Auftraggeber sind natürliche oder juristische Personen und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder dazu andere heranziehen (§ 4 Z 4 DSG). Auftraggeber tragen die Verantwortung dafür, dass der Dienstleister die Daten auch vertragsgemäß, also auch gemäß dem Datenschutzgesetz verwendet (§ 11 DSG).

**Pflichten der Auftraggeber**

Ein Auftraggeber darf einen Dienstleister nur beauftragen wenn

- der Dienstleister die rechtmäßige und sichere Verarbeitung der Daten gewährleisten kann,
- der Auftraggeber und der Dienstleister die zur Datenverarbeitung notwendigen Vereinbarungen treffen (z.B. zu Datensicherheit, Verwendungszweck, Informationsrecht der Betroffenen, Löschung nach Auftragsbeendigung, ...),
- der Auftraggeber sich von die Einhaltung der Vereinbarungen auch wirklich überzeugt.

### 2.4.3 Dienstleister

**Dienstleister**

Auch DienstleisterInnen können natürliche oder juristische Personen sein (z.B. Personengemeinschaft, Gebietskörperschaft, Unternehmen). Sie verarbeiten die Daten, die ihnen überlassen wurden, um eine Dienstleistung zu erbringen (§ 4 Z 5 DSG).

**Abgrenzung von Auftraggeber und Dienstleister**

Entscheidend für die Definition von Dienstleister und Auftraggeber im Sinne des DSG ist, wer über die Datenverarbeitung entscheidet. Wer über die Daten und ihre Verwendung entscheidet, ist Auftraggeber - unabhängig davon, ob Auftraggeber ihre Daten auch gleich selbst verarbeiten, sind sie in beiden Fällen Auftraggeber. Überträgt der Auftraggeber die Durchführung der Datenverarbeitung einem Dienstleister, liegt ein Dienstleisterverhältnis vor.

Die Abgrenzung zwischen Auftraggeber und Dienstleister ist oft schwierig. DienstleisterInnen können zu AuftraggeberInnen werden, wenn sie eigenverantwortlich über die Datenverwendung entscheiden.

Dieses Problem der Unterscheidung stellt sich vor allem in großen Konzernen, in denen Abteilungen für andere Abteilungen oder Konzerngesellschaften Leistungen erbringen. Abgrenzungsprobleme können bei Abteilungen wie Buchhaltung, Personalverwaltung und Controlling entstehen. Es kann beispielsweise vorkommen, dass die Controllingabteilung als selbstständige Auftraggeberin anderen Konzerngesellschaften oder Abteilungen übergeordnet ist. Ebenso verkomplizieren die personellen Verflechtungen und zentralisierten Organisationsstrukturen in multinationalen Konzernen die Sachlage. So sind z.B. oft Personalverwaltung und Controlling im Konzern zentralisiert, die Beschäftigten dieser Abteilungen jedoch in unterschiedlichen Ländern und Konzerngesellschaften angesiedelt. Somit ist es in der Praxis oft höchst aufwendig aus diesen Strukturen die datenschutzrechtlich Verantwortlichen herauszufiltern.

**Pflichten der Dienstleister**

Der Dienstleister hat die Pflicht, die ihm überlassenen Daten nur für den vereinbarten Zweck zu verwenden. Die Weiterleitung an Dritte ist - wenn sie nicht vertraglich vereinbart wurde - ausdrücklich verboten (§ 11 DSG). Die **Rechte der Betroffenen** auf Information, Richtigstellung, Löschung und Widerruf müssen gewahrt bleiben und die dazu nötigen **technischen und organisatorischen Voraussetzungen** müssen geschaffen werden. Nach Beendigung der Dienstleistung müssen alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber übergeben werden oder in dessen Auftrag für ihn weiter aufbewahrt oder **vernichtet** werden.

Die Überlassung und Übermittlung von Daten an Dienstleister muss auf jeden Fall den Grundprinzipien von Datenverwendungen folgen (siehe Kapitel 3).

### 2.4.4 Empfänger oder Dritte

**weitere HandlungsträgerInnen**

Neben den genannten Personengruppen gibt es noch eine Gruppe „Außenstehender", EmpfängerInnen und Dritte. Die österreichische Gesetzgebung definiert diese Personengruppen nicht ausdrücklich, die EU-Richtlinie zum Datenschutz schon.

**Dritte** sind vom Auftraggeber ermächtigt, Daten zu verwenden (z.B. Subunternehmer von Unternehmen, die im Auftrag von Konzernen Datenanwendungen durchführen).

**Empfänger** sind - wie schon der Name sagt - diejenigen, die die Daten erhalten. Manchmal ist in diesem Zusammenhang auch von „Datenimporteuren" die Rede.

### 2.4.5 Informationsverbundsystem

**Eigenschaften des Informationsverbundsystems**

Ein Informationsverbundsystem zeichnet sich dadurch aus, dass Daten durch mehrere Auftraggeber gemeinsam in einer Datenanwendung verwendet werden (§ 4 Z 13 DSG). Jeder Auftraggeber hat dabei auch auf jene Daten im System Zugriff, die von den anderen Auftraggebern zur Verfügung gestellt wurden. In einem Informationsverbundsystem kann jeder Systemteilnehmer Daten einspeichern und sie damit allen anderen Teilnehmern zur Verfügung stellen (z.B. Flugbuchungssysteme, Hotelreservierungssysteme, Unternehmensnetzwerke).

**Meldung eines Informationsverbundsystems**

Jede Datenanwendung in einem Informationsverbundsystem muss der DSK gemeldet werden. Die Meldung kann für alle Beteiligten gemeinsam eingereicht werden und auch der Bescheid ergeht an alle Betreiber des Systems gemeinsam. Derzeit sind bei der DSK vier Informationsverbundsysteme gemeldet. Auch bei vorsichtiger Schätzung kann man davon ausgehen, dass es sich dabei nur um eine geringe Zahl der tatsächlich bestehenden Informationsverbundsysteme in Österreich handelt.

**Pflichten für ein Informationsverbundsystem**

Liegt ein solches Informationsverbundsystem vor sind gewisse Auflagen zu befolgen:

- Ein Informationsverbundsystem darf erst nach Genehmigung in Betrieb genommen werden. Ohne Genehmigung können Verwaltungsstrafen bis zu 10.000 EUR verhängt werden (§ 18 Abs. 2 Z 4 DSG).
- Der Auftraggeber eines Informationsverbundsystems muss dem Datenverarbeitungsregister (DVR) einen Betreiber für das System melden. Dieser Betreiber kann entweder ein Auftraggeber oder ein Dritter sein. Der Betreiber ist verpflichtet jedem/r Betroffenen auf Antrag innerhalb von 12 Wochen alle Auskünfte zu geben, die der/die Betroffene benötigt, um den für die Verarbeitung seiner/ihrer Daten im System verantwortlichen Auftraggeber festzustellen. Der Betreiber haftet für die Datensicherheit (§ 50 Abs. 1 und 2 DSG).
- Jeder einzelne Auftraggeber muss seine/ihre Teilnahme am Informationsverbundsystem gesondert melden. Zulässig ist ein Informationsverbundsystem also nur dann, wenn die Datenübertragung zwischen jedem einzelnen Teilnehmer auch zulässig ist.
- Wird ein Informationsverbundsystem geführt, ohne dass eine entsprechende Meldung an die DSK unter Angabe eines/r Betreibers/in erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

**Checkliste zur Datenweitergabe in einem Informationsverbund**

> Zu welchem Zweck werden Daten weitergegeben?
> Ist es ein berechtigter Zweck?
> Wer erhält die Daten?
> Wurde eine Meldung an das DVR gemacht?
> Wurden die erforderlichen Zustimmungserklärungen eingeholt?
> Hat der Betriebsrat Mitspracherecht (z.B. weil Systeme zur automationsunterstützten Übermittlung von personenbezogenen Daten von MitarbeiterInnen eingeführt werden)?

Wenn ja:

> Wurden mit dem Betriebsrat Vereinbarungen zum Informationsverbundsystem getroffen?
> Besteht ein Anpassungsbedarf in bestehenden Dienstverträgen, Betriebsvereinbarungen, Vereinbarungen mit den MitarbeiterInnen?

# 3) **Grundsätze** bei der Verwendung von Daten

**Prinzip der Rechtmäßigkeit**

Die wesentlichen Prinzipien für Datenverwendung sind im DSG festgelegt (§ 6 DSG).[1]

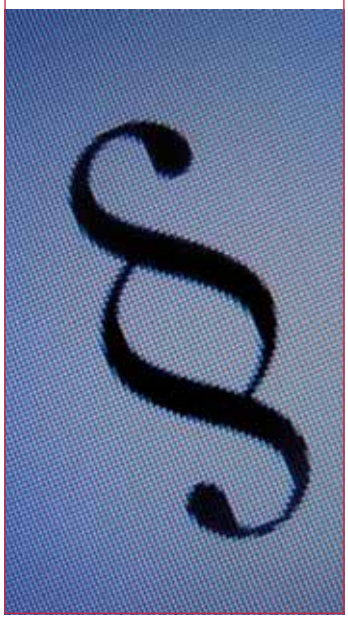
1. Daten dürfen nur nach Treu und Glauben und auf **rechtmäßige Weise** verwendet werden.
   Eine etwas unklare Definition, die als Befolgung sämtlicher Datenschutzbestimmungen und Gesetze sowie der Einhaltung sittlicher Grundsätze zu interpretieren ist. Der/die Betroffene darf über die Umstände des Datengebrauchs seiner/ihrer Daten nicht in die Irre geführt werden.

**Prinzip der Zweckmäßigkeit und Eindeutigkeit**

2. Daten dürfen nur für **festgelegte, eindeutige und rechtmäßige Zwecke** ermittelt und nicht in einer mit diesen Zecken unvereinbaren Weise weiterverwendet werden.
   Unternehmen versuchen aus Profitinteressen möglichst viele und mitunter auch wahllos zusammengestellte Daten ihrer KundInnen und MitarbeiterInnen zu sammeln (data warehouse). Diese Datenbanken werden dann nach vielfältigsten Kriterien und Verknüpfungen durchforstet (data mining) um „maßgeschneiderte KundInnenprofile" zu finden. Diese Art von Datensammelwut ist im Sinne des DSG unzulässig. Der Zweck der Datensammlung muss im Vorhinein genau festgelegt werden. Auch die Weiterverarbeitung der Daten muss mit dem vorher definierten Zweck der Datenermittlung übereinstimmen. Unbestimmte Datensammlungen zur zukünftigen Verwendung stehen im krassen Widerspruch zur eben beschriebenen Zweckbindung.

**Beispiel aus der Praxis**
Ein Unternehmen hat zur Lohnverrechnung verschiedene Daten über die MitarbeiterInnen gespeichert. Nun möchte jemand aus der Human Ressource Abteilung eine spontane Abfrage machen und sucht nach Alter > 45 Jahre, Fehlzeiten > 15 Tage und Leistungsgrad < 110%. Dieses Vorgehen ist datenschutzrechtlich unzulässig und es muss technisch und rechtlich dafür gesorgt werden, dass es nicht passieren kann.

3. Daten dürfen nur verwendet werden, sofern sie **für den Zweck der Datenanwendung wesentlich** sind, und über diesen Zweck nicht hinausgehen.
   Man kann sich daran orientieren, dass bei der Verwendung der Daten immer ein „Minimalprinzip" eingehalten werden muss, d.h. es muss geklärt werden, ob die Vorgehensweise tatsächlich das am wenigsten in die Rechte der Betroffenen eingreifende Verfahren ist, um das gewünschte Ziel zu erreichen. Der Eingriff in die Privatsphäre muss auf ein Minimum beschränkt sein. Es müssen die „gelindesten zur Verfügung stehenden Mittel" zur Datenverarbeitung eingesetzt werden (§ 7 Abs. 3 DSG).



Dieses Prinzip bezieht sich ebenfalls auf die Zweckmäßigkeit und soll den Umfang der erfassten Daten beschränken und die überbordende Datensammelleidenschaft sowie die Technophilie in vielen HR-Abteilungen hintanhalten.

**Beispiel aus der Praxis**
Eine japanische Konzernzentrale möchte in allen europäischen Konzerntöchtern Zugriff auf die Personaldatenbanken der lokalen HR-Abteilungen haben. Der angegebene Zweck ihrer Anfrage ist jedoch nur den head-count (Beschäftigtenzahl) der in Europa beschäftigten MitarbeiterInnen zu erfahren. Nach dem DSG ist die österreichische HR-Abteilung nicht verpflichtet den Zugang zu gewähren, da eine einfache Auskunft über die Gesamtzahl der Beschäftigten für diesen Zweck völlig ausreichend ist. Daten wie Adresse, Geburtsdatum etc. müssen dazu nicht übermittelt werden.

[1] Artikel 6 der Datenschutzrichtlinie der EU enthält sinngemäß dieselben Regelungen.

4. Daten dürfen nur in der Art und Weise verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, falls notwendig, auf den neuesten Stand gebracht sind.
   Dieser Grundsatz der sachlichen Richtigkeit bedeutet, dass Daten inhaltlich richtig ermittelt bzw. gespeichert werden müssen. Der/die ArbeitgeberIn hat dafür zu sorgen, dass das Geburtsdatum oder das Entgelt der Beschäftigten korrekt ermittelt und gespeichert wird. Ist dies nicht der Fall, können die Betroffenen Richtigstellung oder Löschung beantragen und auch durchsetzen (siehe weiter unten in diesem Kapitel).

**Prinzip der Richtigkeit und der Aktualität**

5. Daten dürfen nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist, eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften (z.B. Buchhaltung, Steuer) ergeben.
   Das DSG kennt keine vorgegebenen Fristen zur Datenspeicherung, denn Daten dürfen nur solange in personenbezogener Form aufbewahrt werden, als dies zum Erreichen des Zweckes der Ermittlung und Verarbeitung notwendig ist.
   Eine Ausnahme bilden die Standard- und Musteranwendungen da dort Ereignisse oder gesetzliche und archivrechtliche Vorschriften die Speicherfrist begrenzen können (siehe auch Kapitel 4.1).

**Prinzip der kürzesten Dauer**

6. Als einer der wichtigsten Grundsätze gilt außerdem der **„Anspruch auf Geheimhaltung"**. Nachdem der Gesetzgeber ihn an allererster Stelle nennt (§1 Abs. 1 DSG) kann man getrost davon ausgehen, dass er auch dementsprechend bedeutend ist. Allerdings gibt es jede Menge Ausnahmen vom Recht auf Geheimhaltung personenbezogener Daten - polemisch formuliert: ein Großteil des DSG ist den Ausnahmen gewidmet. Grob zusammengefasst ist das Recht auf Geheimhaltung eingeschränkt wenn:
   - persönlich der Datenverwendung zugestimmt wird,
   - Gesetze die Datenverwendung vorsehen (der Gesetzgeber kann sich also selbst seine Ausnahmen schaffen),
   - lebenswichtige Interessen der Betroffenen gefährdet sind oder wenn
   - überwiegende Interessen Dritter oder Auftraggeber gewahrt werden müssen (auch hier also eine Art Generalklausel, die relativ weiten Interpretationsspielraum lässt).

**Geheimhaltungsprinzip**

Datenschutz ist aber auch kein Recht mit absolutem Vorrang gegenüber anderen Rechten und Freiheiten. Man muss den Schutz von Daten und Privatsphäre gegen andere schutzwürdige Interessen abwägen. Es muss beispielsweise abgewogen werden, ob die Eigentumsrechte des/der Arbeitgebers/in am PC überwiegen, oder ob das Briefgeheimnis der ArbeitnehmerInnen überwiegt. Ein weiteres Bespiel wäre Staatsschutz versus Medienfreiheit.

**Abwägen zwischen den Rechten**

## Betroffenenrechte

„Arbeitnehmer geben ihr Recht auf Schutz der Privatsphäre nicht allmorgendlich am Fabrikstor oder an der Bürotür ab." - hält die EU-Datenschutzgruppe fest.

**wichtigste Betroffenenrechte**

Diejenigen, deren Daten verarbeitet werden, haben Recht auf:

- Information über Zweck und Gegenstand der Datenanwendung sowie Empfänger der Daten - auch wenn ein Datenverarbeiter keine personenbezogenen Daten von Betroffenen vorliegen hat, sollte dieser Umstand den Betroffenen mitgeteilt werden, so die EU-Datenschutzgruppe,
- Auskunft über Zweck und Gegenstand der Datenanwendung sowie Empfänger der Daten ohne unzumutbare Verzögerung oder Kosten,
- Berichtigung falscher Daten,
- Löschung und/oder Sperrung falscher Daten bzw. widerrechtlich erfasster Daten,
- Widerruf einmal gegebener Zustimmungen zur Datenverwendung,

**Pflichten der Auftraggeber gegenüber den Betroffenen**

- Vertraulichkeit und Sicherheit der Datenanwendung,
- Herkunft der Daten,
- logischer Aufbau der Datenanwendung - so sie automatisiert erfolgt.
- Ferner muss die Auskunft in verständlicher Form gegeben werden.

Aus den Betroffenenrechten ergibt sich zugleich ein eindeutiger Arbeitsauftrag an die Auftraggeber von Datenverarbeitungen: Informationspflicht, Auskunftspflicht, Berichtigungspflicht, Löschungspflicht bei falschen Daten und Pflicht zur Gewährung des Widerrufrechts. Auch die Meldung bei der Datenschutzkommission (siehe Kapitel 5) - so sie für die jeweilige Datenanwendung gesetzlich vorgesehen ist - gehört zu dem **Mindestmaß an Datenschutz**, der von dem/der ArbeitgeberIn eingehalten werden sollte. Viele Datenverwendungen sind zwar inhaltlich legitim, verstoßen aber deshalb gegen österreichisches Recht, weil die Minimalanforderungen an die Transparenz (Information der Betroffenen, Meldung bei der Datenschutzkommission) nicht erfüllt sind.

**Zustimmung der Betroffenen**

Möchte eine Firma sensible personenbezogene MitarbeiterInnen-Daten transferieren (z.B. Religionsbekenntnis), ist die Zustimmung **jedes/r einzelneN MitarbeiterIn** nach dem DSG einzuholen. Das DSG verlangt, dass die Zustimmungserklärung:

- frei,
- ohne Zwang und
- in Kenntnis der Sachlage
- für den konkreten Fall

abgegeben wird (§4 Z 14 DSG). [2]

**fallbezogen**

Die Wortwahl **„für den konkreten Fall"** bedeutet, dass jede Zustimmung nur für jeweils eine Datenanwendung gültig ist und keine „Blanko-Zustimmung" oder automatisierte Zustimmung von den ArbeitnehmerInnen eingeholt werden kann

**informiert**

**„In Kenntnis der Sachlage"** bedeutet, dass die ArbeitnehmerInnen Bescheid wissen, was mit ihren Daten passieren soll. Der/die ArbeitgeberIn hat eine Informationspflicht gegenüber den MitarbeiterInnen. Er/sie muss Auskunft darüber geben, welche Daten zu welchem Zweck verarbeitet werden, wer unter welchen Bedingungen Zugriff auf die Daten hat und wann sie wieder gelöscht werden.

**freiwillig**

Die Artikel-29-Datenschutzgruppe der EU ist der Ansicht, dass: „Die Einwilligung der betroffenen Person (…) nur in den Fällen in Anspruch genommen werden [sollte], in denen der Beschäftigte eine echte Wahl hat und seine Einwilligung zu einem späteren Zeitpunkt widerrufen kann, ohne dass ihm daraus Nachteile erwachsen." Sind mit einer Nicht-Einwilligung tatsächliche oder potentielle Nachteile verbunden, ist die EU-Datenschutzgruppe der Meinung, dass die **Freiwilligkeit** nicht gegeben ist und somit die Zustimmung ungültig ist. Auch gesetzt den Fall, dass eine Nicht-Einwilligung gar nicht möglich ist, kann man nicht von „Freiwilligkeit" ausgehen.

[2] Auch die europäische DSRL enthält eine solche Formulierung (Art. 2 Buchstabe h DSRL). Auch die Judikatur zeigt sich bisweilen recht eindeutig im Umgang mit „Zustimmungserklärungen". Der OGH hob bereits mehrmals derartige Klauseln auf. Bisher vor allem im Zusammenhang mit Kundendaten: vgl. 4Ob28/01y; 6Ob16/01y; 4Ob221/06p.


**Aus der Praxis**
Viele Unternehmen holen sich die „Zustimmung" der Angestellten bereits beim Einstellungsgespräch. Zusammen mit dem Arbeitsvertrag wird den künftigen MitarbeiterInnen eine Zustimmungserklärung für die „firmeninterne" Datenverwendung vorgelegt. Dass damit auch der Datentransfer ins Ausland, die Verknüpfung von Daten, etc. gemeint sein können, ist nur informierten Personen bekannt. Probleme entstehen wenn die Einwilligung Einstellungsvoraussetzung ist. Der/die ArbeitnehmerIn hat theoretisch das Recht, die Einwilligung zu verweigern, aber er/sie muss in diesem Fall damit rechnen, dass er/sie die Chance auf eine bestimmte Stelle verliert. Unter solchen Umständen wird die Einwilligung nicht freiwillig erteilt und ist daher nicht gültig.
Der/die Betriebsrat/rätin sollte eine solche Praxis möglichst unterbinden, die MitarbeiterInnen gegen solche Vorgehensweisen sensibilisieren und mit der Geschäftsführung statt dessen eine (Konzern-) Betriebsvereinbarung zum Datenschutz abschließen.

Die Verarbeitung personenbezogener Daten kann allerdings auch trotz persönlicher Zustimmung unzulässig sein. **„Die Einwilligung der betroffenen Person ist nie ein vorrangiges Kriterium."** - stellt die Artikel-29-Datenschutzgruppe fest. Wenn beispielsweise kein angemessener Zweck vorliegt, die Datensicherheit nicht eingehalten wird oder die Datenverarbeitung über das erforderliche Mindestmaß hinausgeht, entspricht die Datenanwendung trotz persönlicher Zustimmung nicht der Datenschutz-Richtlinie der EU.

**Praxisbeispiel der Artikel-29-Datenschutzgruppe**
Ein Arbeitgeber kann ein berechtigtes Interesse an der Kontrolle der Leistung seiner Büroangestellten mit Hilfe der Erfassung ihres Arbeitsoutputs (z. B. Zahl der Vorgänge, die ein Beschäftigter bearbeitet hat, oder Zahl der entgegengenommenen Telefonanrufe usw.) haben. In diesem Fall muss der Arbeitgeber nicht nur die nachstehenden Grundsätze, insbesondere das Gebot der Verhältnismäßigkeit, beachten, er darf diese Art von Daten auch nur dann verarbeiten, wenn die Arbeitnehmer ordnungsgemäß informiert worden sind. Hat eine solche Kontrolle ohne ordnungsgemäße Unterrichtung der Beschäftigten stattgefunden, verstößt die Verarbeitung der so gewonnen Beschäftigtendaten gegen die Vorschriften der Richtlinie 95/46/EG.

**Recht auf Löschung**

Die **Löschung** ist ein wesentliches Element zur Durchsetzung der Betroffenenrechte. Im Sinne des Datenschutzgesetzes dürfen Daten nur für festgelegte Zwecke ermittelt, nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden und nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist (Ausnahme: gesetzliche archivrechtliche Vorschriften).

**Pflicht zur Richtigstellung und Löschung**

In weiterer Folge beinhaltet dies auch die Verpflichtung des Auftraggebers zur Richtigstellung und Löschung (u.a. §§ 27 und 11), wenn die Daten unrichtig sind oder unzulässig verarbeitet worden sind oder der/die Betroffene dies begründet verlangt. Die Betroffenen haben ein dezidiertes Recht auf Richtigstellung ihrer Daten (§ 27 DSG). Kommt der Auftraggeber der Richtigstellung der Daten auf Verlangen nicht nach, kann dies eine Verwaltungsstrafe in der Höhe von 9.000 EUR nach sich ziehen.

**Aufgabe des Betriebsrates**

Wesentlich für BetriebsrätInnen und/oder Datenschutzbeauftragte ist daher, im Anlassfall genau auf den konkreten Auftrag oder vorliegende Zustimmungserklärungen der Person zu schauen, deren Daten erfasst, verwendet usw. werden sollen sowie den konkreten Zweck der Datenerfassung und Datenverwendung und auch die Argumentation zu hinterfragen, warum welche Daten wie verarbeitet, übermittelt, nicht gelöscht usw. werden sollen.

**Beispiel aus der Praxis**

BewerberInnen richten ein Bewerbungsschreiben inklusive Lebenslauf, Arbeitszeugnissen, etc. für eine bestimmte Stelle an ein Unternehmen. Dieses Unternehmen wählt dieseN BewerberIn zwar nicht aus, speichert aber die Daten dauerhaft weiter.

Der Betriebsrätin kam das nicht ganz einwandfrei vor. Sie begann Erkundigungen einzuziehen. Rechercheergebnis war, dass es zwar keine Zuständigkeit des Betriebsrats im Sinne des ArbvG für BewerberInnen gibt, wenn diese Bewerbungen nicht in einem Beschäftigungsverhältnis münden. Andererseits ist aber das Datenschutzgesetz anzuwenden. Der Zweck der Daten liegt ausschließlich in der konkreten Bewerbung. Daten dürfen generell nur gemäß ihrem Zweck und bis zur Beendigung der Beziehung mit dem Betroffenen gespeichert werden. Darüber hinaus darf nur aufbewahrt werden, solange gesetzliche Aufbewahrungsfristen bestehen oder Rechtsansprüche aus dem Arbeitsverhältnis geltend gemacht werden können. Wenn es jedoch kein Arbeitsverhältnis gibt, ist eine dauerhafte Speicherung nicht in Ordnung. Daten der Bewerbung dürfen nicht ohne speziellen Auftrag des/der Bewerbers/in an andere Unternehmen/Dienstleister (z.B. im Konzern) übermittelt werden.

# 4) Wo geht's lang?
## Das Prozedere beim Datenschutz

**komplexe Vorgehensweise beim Datentransfer**

Um Datenanwendungen durchführen zu dürfen, müssen die Auftraggeber bestimmte Schritte befolgen. Je nachdem, welche Daten wofür verwendet werden sollen und wohin sie geschickt werden sollen, müssen unterschiedliche Regelungen eingehalten werden. Manche Anwendungen können ohne Meldung oder Genehmigung der Datenschutzkommission gemacht werden, andere wiederum unterliegen der Melde- und/oder Genehmigungspflicht und wieder andere müssen einer so genannten „Vorabkontrolle" unterzogen werden.

Zusätzlich zum Datenschutzgesetz, das die Bestimmungen zu den persönlichen Zustimmungspflichten enthält, muss aber noch das Arbeitsverfassungsgesetz berücksichtigt werden, dass die Bestimmungen zu den Mitbestimmungsrechten des Betriebsrates enthält. Die beiden Gesetzesmaterien ersetzen einander nicht. Es kann nicht sein, dass die Zustimmung Einzelner, zu einem Ausschluss des Betriebsrates führt oder dass der Betriebsrat für die ganze Belegschaft zustimmt und dabei datenschutzrechtliche Grundvoraussetzungen übergeht.

**Datenübermittlung ohne Genehmigung und bei Rot über die Kreuzung - beides kann gut gehen, muss aber nicht.**

**Als grober Anhaltspunkt gilt:**

**Übermittlung und Überlassung sensibler Date**

**Sensible Daten** dürfen generell **nicht übermittel oder überlassen** werden. Dies ist nur dann möglich, wenn die Betroffenen (siehe Kapitel 2.4.1) zugestimmt haben, die Datenschutzkommission (siehe Kapitel 5) den Datentransfer genehmigt und eine Vorabkontrolle durchgeführt hat.

**Übermittlung und Überlassung personenbezogener Daten**

Bei **personenbezogenen Daten** (siehe Kapitel 2.1.2) kommt es darauf an, ob sie innerhalb Österreichs und des EU-Raums übermittelt werden, oder ob sie die Schengen-Grenzen überschreiten. Ihre Verarbeitung innerhalb von Österreich und innerhalb des EU- und EWR-Raumes ist zulässig. Die Übermittlung ist meldepflichtig - die Ausnahmen innerhalb der EU sind in § 17 Abs. 2 und 3 DSG festgelegt. Innerhalb der EU gibt es jedoch keine Genehmigungspflicht. Die Überlassung und Übermittlung an Drittstaaten muss genehmigt werden - Ausnahmen bestimmt der § 12 Abs. 3 und 4 DSG.

**Vorabkontrolle**

Eine Vorabkontrolle muss bei **sensiblen Daten** und bei **Informationsverbundsystemen** (siehe Kapitel 2.4.5) durchgeführt werden. Die Vorabkontrolle ist ein erweitertes Genehmigungsverfahren, bei dem die Daten erst nach einer längeren Sperrfrist übermittelt werden dürfen.

## 4.1 Standard- und Musteranwendung

**genehmigungsfreier Datentransfer**

Bei bestimmten allgemein gebräuchlichen Datenanwendungen besteht keine bzw. vereinfachte Meldepflicht und keine Genehmigungspflicht. Welche Anwendungen das sind, hat der/die BundeskanzlerIn mit der so genannten Standard- und Musterverordnung festgelegt. Diese Standard- oder Musteranwendungen listen haargenau auf, **welche Datenerhebungen für welche Datenanwendungen mit welchen Empfängerkreisen** auch ohne Meldung bei der Datenschutzkommission erlaubt sind (z.B. SA 002 BGBl. II Nr. 232/2003; Personalverwaltung für privatrechtliche Dienstverhältnisse). Zu den Standardanwendungen zählen z.B. Reisekostenabrechnung, Lohn- und Gehaltsverrechnung oder Videoüberwachung in bestimmten Betrieben (z.B. Banken, Trafiken, Tankstellen, Juweliere). Nicht dazu zählen z.B. die Verwaltung von BewerberInnen-Dateien oder die Aus- und Weiterbildungsverwaltung.


Meist geht es bei diesen Anwendungen um Stammdaten der MitarbeiterInnen, die die schutzwürdigen Geheimhaltungsinteressen nicht gefährden. Die Empfängergruppe für die jeweiligen Daten ist genau in der Standardanwendung aufgelistet (z.B. Personalabteilung, Sozialversicherung, Finanzamt, Geschäftsführung,...) und muss mit den tatsächlichen Empfängern auch übereinstimmen. Man kann beispielsweise nicht mehr von einer Standardanwendung „Personalverwaltung für privatrechtliche Dienstverhältnisse" ausgehen, wenn der an die Mitarbeiterkasse eingezahlte Beitrag nicht nur an die Mitarbeitervorsorgekasse, das Finanzamt und Sozialversicherungsträger weitergegeben wird (diese Gruppen sind in der Standardanwendung 002 vorgesehen), sondern zusätzlich automatisch an andere Empfänger (z.B. Banken).

**Standardanwendungen (SA) sind weder genehmigungs- noch meldepflichtig. Musteranwendungen (MA) sind meldepflichtig, aber nicht genehmigungspflichtig.** Eine Musteranwendung wird mittels vorgefertigtem Formular (Formblatt 3) bei der DSK eingereicht, stellt also eine Erleichterung bei der Meldepflicht dar. Für Betriebe ist die gebräuchlichste Musteranwendung MA 002 „Zutrittskontrollsysteme".

## 4.2 Meldepflicht

**Verarbeitung personenbezogener Daten muss gemeldet werden**

Bei der Verwendung von personenbezogenen Daten besteht - außer bei den so genannten Standard- und Musteranwendungen - Meldepflicht. Das heißt, die Datenschutzkommission muss vor der Verwendung informiert werden (§ 17 DSG). Die Datenschutzkommission trägt dann die Datenverwendung in das Datenverarbeitungsregister (DVR) ein.

**formale Meldung bei der DSK**

Damit eine Datenverwendung rechtmäßig ist, muss der Auftraggeber zunächst seine eigenen Stammdaten melden. Meist ist das bereits bei der Gründung der Firma geschehen, weil jedes Unternehmen, jeder Verein, jede Organisation die Nummer aus dem Datenverarbeitungsregister für das tägliche Geschäft fast immer benötigt. Die einmal gemeldeten Stammdaten müssen immer aktuell gehalten werden. Das DVR wird mit 2012 über eine online-Datenbank geführt werden. Die Eintragung sowie die Einsicht erfolgt über das Internet. Die Datenanwendung selbst wird dann vor ihrer Aufnahme beim DVR gemeldet. Die Meldung ist einigermaßen umfangreich und umfasst (§ 19 Abs. 1):

- Daten zum Auftraggeber (also die Stammdaten und DVR-Nummer der Firma sowie ihre rechtliche Vertretung),
- allfällige Bertreiber der Datenanwendung (z.B. Informationsverbundsystem),
- Nachweis der gesetzlichen Zuständigkeit oder die rechtliche Befugnis zur Datenverarbeitung (z.B. Gewerbeberechtigung, Konzession, Vereinsstatuten etc. - siehe § 7 Abs. 1 DSG),
- Zweck der Datenanwendung und ihre Rechtsgrundlagen,
- betroffene Personen (z.B. Mitarbeiter, Kunden, Lieferanten, etc.),
- Datenarten (z.B. Namen der Konzernunternehmen und deren Sitz),
- Empfängerkreise (Werden z.B. Daten von ArbeitnehmerInnen eines österreichischen Tochterunternehmens an die Konzernmutter in Frankreich und an die HR-Abteilung in Deutschland übermittelt, müssen beide in der Meldung angegeben werden.),
- allfällige Genehmigung der Datenschutzkommission (z.B. bei einer Übermittlung von Daten in ein Land außerhalb der EU),
- Angaben über Datensicherheitsmaßnahmen (Diese sind mittels eigenem Formular zu melden; § 14 Abs. 2 DSG.).

**Inbetriebnahme von Datenanwendungen**

Die Datenanwendung darf **sofort nach der Meldung** in vollem Umfang in Betrieb gehen. Ist die Standardanwendung, die Musteranwendung oder die Meldung inneren Angelegenheiten anerkannter Kirchen und Religionsgemeinschaften erledigt, kann die Datenverwendung beginnen (§ 18 Abs. 1 und 2 DSG).

Falls sensible Daten verwendet werden, falls Daten zur Kreditwürdigkeit von Personen verwendet werden, falls strafrechtlich relevante Daten verwendet werden (z.B. Vorstrafen, Leumundszeugnisse), falls Gesundheitsdaten jenseits von Standardanwendungen verwendet werden sollen und falls der Auftraggeber Daten in einem Informationsverbundsystem verwendet möchte, muss die DSK die Anwendung erst einmal prüfen (§18 Abs. 2 DSG). Diese so genannte „Vorabkontrolle" ist ein ausführliches Genehmigungsverfahren.

Die DSK muss alle Meldungen **innerhalb von zwei Monaten prüfen** (§ 20 Abs. 1 DSG). Kommt von der DSK innerhalb von zwei Monaten kein Auftrag zur Abänderung der Meldung, kann die Datenanwendung als gemeldet betrachtet werden und mit der Verwendung begonnen werden. Ausgenommen von der Meldepflicht an die DSK sind Datentransfers ins Ausland, bei denen die Daten (§ 12 DSG):

**Ausnahmen von der allgemeinen Meldepflicht**

- öffentlich zugänglich sind (z.B. Telefonbuch),
- im Inland bereits zulässigerweise veröffentlicht wurden,
- wichtige öffentliche Interessen betreffen (z.B. Terrorbekämpfung),
- aufgrund von Gesetzen eingeholt und übermittelt werden müssen (z.B. Sozialversicherungsnummer an die Sozialversicherung),
- anonymisiert wurden, also nicht mehr personenbezogen sind,
- aufgrund der ausdrücklichen Zustimmung der Betroffenen übermittelt werden,
- lebenswichtige Interessen einer Person bestehen.

**Strafen**

**Eine Verletzung der Meldepflicht kann mit einer Verwaltungsstrafe von bis zu EUR 10.000,- geahndet werden.**

**strategische Mitsprache des Betriebsrates**

Reicht ein Unternehmen eine Datenanwendung bei der DSK ein, so prüft diese aller Wahrscheinlichkeit nach, ob eine Betriebsvereinbarung zum Datenschutz/-transfer vorliegt. Befürwortet der/die Betriebsrat/rätn das Vorhaben, dass bestimmte personenbezogene Daten den Betrieb verlassen und an Dritte überlassen oder übermittelt werden, so ist er/sie gut beraten, vor diesem Datentransfer eine Betriebsvereinbarung abzuschließen.

Eine Meldung an die DSK ist Voraussetzung dafür, dass ein Transfer sensibler Daten legal durchgeführt werden kann. Der/die Betriebsrat/rätin hat somit die Möglichkeit, seine/ihre Zustimmung zum Datentransfer davon abhängig machen, ob eine solche Meldung bereits erfolgt ist. Die Geschäftsführung muss vorweisen, dass die Genehmigung der DSK vorliegt.Allerdings ersetzt eine Zustimmung der DSK nicht zwangsläufig eine Zustimmung des Betriebsrates aufgrund des ArbVG. Umgekehrt führt das Vorliegen einer BV nicht automatisch dazu, dass der Datentransfer von der DSK genehmigt werden kann.

## 4.3 Genehmigungspflicht

**Verarbeitung sensibler Daten muss genehmigt werden**

**Sensible Daten** oder besonders **schutzwürdige Daten** dürfen in keinem Fall ohne Meldung und Genehmigung verwendet werden! **Informationsverbundsysteme** müssen ebenfalls von der DSK genehmigt werden. Sowohl sensible Daten als auch Datenverwendungen in Informationsverbundsystemen unterliegen zusätzlich der Vorabkontrolle.

**Prüfung beim Transfer sensibler Daten ins Ausland**

Sollen sensible Daten ins Ausland übermittelt werden, dann muss die DSK innerhalb der **zwei Monate** entscheiden, ob und wenn ja welche Nachbesserungen vorgenommen werden müssen. Und die DSK muss auch festlegen, ob und in welchem Ausmaß der Datentransfer bereits durchgeführt werden darf.

Die DSK muss ihren Bescheid **innerhalb von sechs Monaten ausstellen** (§ 73 AVG - Allgemeines Verwaltungsverfahrensgesetz). Gegen den Bescheid der DSK ist kein weiteres Rechtsmittel zulässig. Es kann höchstens eine der handelnden Personen zum Verwaltungsgerichtshof gehen.

**Datentransfer in Dritt-Staaten ist genehmigungspflichtig**

Außerdem ist die Übermittlung von Daten in EU-Drittstaaten ohne angemessenes Datenschutzniveau genehmigungspflichtig. Ausnahmen bestätigen auch hier die Regel; so genannte „Standardvertragsklauseln" und „Safe-Harbor-Richtlinien" vereinfachen den Datentransfer (siehe Kapitel 7.2.1).

Die DSG-Novelle 2010 hat einige Klarstellungen zur Verwendung von Videoaufzeichnungen gebracht (Abschnitt 9a, §§ 50a – 50e). Die Genehmigungspflicht liegt dann nicht vor, wenn Videoaufnahmen ausschließlich in Echtzeit gemacht werden, wenn ausschließlich analoge Speichermedien verwendet werden oder wenn ein Code zur Einsicht in die Aufnahmen geschaffen wird, dessen einziger Schlüssel bei der Datenschutzkommission hinterlegt wird, sodass ohne deren Zustimmung kein Datenzugriff möglich ist. Alle anderen Videokameras sind nach wie vor genehmigungspflichtig.

**Kosten**

**Sowohl Meldung als auch Genehmigung bei der DSK sind gratis.**

# 5) Wer ist zuständig?
## Die Datenschutzkommission

**Aufgaben**

Jede automationsunterstützte Datenanwendung und jeder Datentransfer muss der Datenschutzkommission (DSK) gemeldet werden (siehe Kapitel 4.2 und 4.3) - so es sich nicht um eine so genannte „Standard- oder Musteranwendung" handelt (siehe Kapitel 4.1). Die ARGE-Daten, Österreichs erste Ansprechstelle in punkto kritischem Datenschutz, schätzt, dass dies nur bei 20 % der Anwendungen tatsächlich der Fall ist. **80 % der betrieblichen Datenverwendungen werden nicht an die Datenschutzkommission gemeldet!**

Die DSK registriert jede automationsunterstützte Speicherung, Verarbeitung, Verknüpfung, etc. von Daten im österreichischen Datenverarbeitungsregister (DVR) und vergibt Registrierungsnummern (DVR-Nr.) an die Unternehmen/Vereine/Betriebe. Ist das Land, in das die Daten übermittelt werden sollen, außerhalb der EU bzw. des EWR (also per EU-Definition ein Land ohne angemessenes Datenschutzniveau) muss die DSK den Transfer überprüfen und genehmigen. (Ausnahmen sind Standardvertragsklauseln und Safe-Harbor-Richtlinien, siehe Kapitel 7.2.1.)

**Handlungsmöglichkeiten**

Die DSK hat folgende Möglichkeiten auf Anträge zum Datentransfer zu reagieren:

- Antragsmäßige Genehmigung
- Genehmigung unter Bedingungen/Auflagen
- Teilweise Genehmigung und Abweisung des übrigen Teils
- Abweisung des gesamten Antrags

**Beispiel aus dem öffentlichen Dienst**
Die MitarbeiterInnen einer Behörde müssen Arbeitsbeginn und Arbeitsende „zeitnah", also möglichst bald, in ein Programm eingeben. Zur „Plausibilitätsprüfung" wurde zusätzlich protokolliert, wann die MitarbeiterInnen in das Programm eingestiegen sind. Protokolle und Eintragungen der MitarbeiterInnen wurden an die AbteilungsleiterInnen übermittelt. Die Datenschutzkommission entschied, dass diese Vorgehensweise ungesetzlich ist. Die Aufzeichnung der Protokolldaten ist zur Dienstaufsicht und zur Arbeitszeitkontrolle ungeeignet. Ein anderer Verwendungszweck wurde nicht angegeben und daher sind die Daten gem. § 27 Abs. 1 Z 1 DSG zu löschen.

**Beispiel aus der Automobilindustrie**
Als Einstellungstest wurden die so genannten „Massachusetts-Tests" mit ausgeklügelten psychologischen Bewertungsverfahren eingeführt. Der Einstellungstest ist nach § 96 ArbVG zustimmungspflichtig. Der Betriebsrat regte an, diese Datenerfassung von der DSK registrieren zu lassen. Die DSK hat die Anwendung des Tests im Bewerbungsverfahren untersagt.

**Charakteristika**

Die DSK ist im Bundeskanzleramt angesiedelt. Sie hat sowohl Funktionen des Gesetzesvollzugs als auch der Kontrolle. Somit ist das System der Gewaltentrennung bei der DSK eher schwach ausgeprägt.

**europäischer Vergleich**

Im europäischen Vergleich zählt die personelle Ausstattung der österreichischen DSK 2007 zu den Schlusslichtern. Durchschnittlich sind 45 Personen in den europäischen Datenschutzkontrollstellen angestellt - in Österreich sind es 20. Damit steht Österreich an 22. Stelle der 27 EU-Staaten. Betrachtet man die Sache in Relation zur Zahl der EinwohnerInnen, rutscht Österreich an die 23. Stelle. Und wenn man sich nur die Staaten mit vergleichbaren Einwohnerzahlen ansieht (fünf bis zehn Millionen), ist nur mehr Portugal hinter Österreich, das Platz zehn von elf einnimmt. Die tschechische Republik mit 85 Vollzeitstellen liegt bei dieser Liste auf Platz eins. Im Vergleich mit 2005 ist Österreich um drei Plätze nach hinten gewandert. **Die österreichische Datenschutzkommission ist im EU-Vergleich unterbesetzt!**

# 6) **Alles ist machbar!?** Technische Überwachungsmaßnahmen

**Modeerscheinung**

Vor zehn Jahren galt es als Nonplusultra im Datensicherheitsmanagement dezentrale Einheiten auf kleinen Rechnern zu schaffen. Derzeit liegt der Großrechner im Trend. Der technische Datenschutz unterliegt also temporären Schwankungen, die sich in etwa alle zehn Jahre ändern.

**Kapazitäten des Großrechners**

Momentan werden Daten wieder im zentralen, alles umfassenden Verbund konzentriert. Einmal damit angefangen, ergibt sich ein gewisser Sachzwang zur Zentralisierung, die „economy of scales" schlägt zu, d.h. je mehr Daten verarbeitet werden, desto besser ist das Großrechner ausgenutzt. Und genutzt werden muss er, weil er in der Errichtung einiges gekostet hat. Alleine die Infrastruktur für solche Großprojekte kann sich sehen lassen; bautechnische Maßnahmen gegen jegliche Umweltschäden, wärmetechnische Maßnahmen um die Erhitzung der Geräte zu vermeiden, energietechnische Maßnahmen um den enormen Stromverbrauch für das alles sicher zu stellen, etc. Klar, dass man hier so viele Daten wie möglich lagern und verarbeiten möchte - ist doch logisch, oder?

**Zweck vorhanden?**

Außerdem werden Unmengen von Daten gespeichert und/oder verarbeitet, da es einen hohen technischen Aufwand bedeuten würde, nur jene Daten auszusortieren, die für das Unternehmen tatsächlich von Bedeutung sind. In Bezug auf die persönlichen Daten von MitarbeiterInnen ist ein solches Vorgehen aber zu bekämpfen. Es muss klar ersichtlich sein, welche Daten zu welchem Zweck aufgehoben werden, wie sie weiter verarbeitet werden, wer Zugriff darauf hat, u.s.w. (siehe „Fragen an die Geschäftsführung" im Kapitel 8.2).

**Überwachung international**

Die technischen Möglichkeiten zur detaillierten Datenaufzeichnung bestehen nicht nur - sie werden auch genutzt. Leider existiert in Österreich keine Aufzeichnung darüber, wie viele Firmen Personaldaten auf welche Art bereits elektronisch verarbeiten. In den USA ist beispielsweise bekannt, dass 2001 63 % der Firmen die von ihren MitarbeiterInnen besuchten Websites überwachen, 36 % Emails speichern und prüfen und 15 % der Unternehmen die Arbeitsleistung der MitarbeiterInnen per Video aufzeichnen. Die Gefahr ist gegeben, dass die Daten nicht nur aufgezeichnet und bewertet werden, sondern auch noch konzernweit mit denen anderer MitarbeiterInnen verknüpft werden.

**Erkennungsmerkmale**

**Woran erkennt man, dass internationale Datentransfers auf der Tagesordnung stehen?**

Wenn es „gut" gemacht wird - gar nicht! Einzelne können anhand technischer Ursachenforschung meist nicht erkennen, was mit den personenbezogenen Daten tatsächlich passiert.

Wenn folgende Fragen aber mit ja beantwortet werden können, ist es sehr wahrscheinlich, dass die Daten konzernweit - zumindest - gespeichert werden.

- Existiert ein internationales Telefonbuch für sämtliche MitarbeiterInnen?
- Können sie sich an jedem beliebigen Standort des Konzerns mit ihren persönlichem Profil einloggen?
- Arbeiten sie bei internationalen Kooperationen über einen Server und können daher sehr rasch und unkompliziert Daten übermitteln?

**Risiko**

Je mehr Daten über Informations- und Kommunikationstechnologie erfasst, gespeichert und verarbeitet werden, desto höher ist auch der Schaden im Falle eines Missbrauchs. Sicherheitseinrichtungen verhindern zwar das unbefugte Eindringen in Datensysteme, aber wenn einmal jemand das System gehackt hat, ist die gewonnene Datenmenge unendlich und den Missbrauchsmöglichkeiten sind keine Grenzen gesetzt.

**Beispiel aus der staatlichen Verwaltung**

Die deutschen Zeitungen „Die Zeit“ und „Der Spiegel“ berichteten im Juli 2007:
„Estland mit seinen knapp anderthalb Millionen Einwohnern gilt als eine der vernetztesten Gesellschaften Europas und Pionier der elektronischen Verwaltung. Bei den letzten Parlamentswahlen konnten die Bürger ihre Stimme online abgeben - eine Weltpremiere. Das macht das Land auch besonders verletzlich.“
„Von einem Cyberkrieg war bereits in Estland die Rede - im Paradeland für den elektronischen Fortschritt. Die Angreifer starteten im April dieses Jahres ihre Attacken. Betroffen waren Behörden und Unternehmen gleichermaßen. Sie wurden mit einer Flut unsinniger Anfragen überschwemmt - bis die Rechner zusammenbrachen.“ Die Folgen eines Ausfalls für ein ganzes Land, dessen staatliche Administration gänzlich auf Internet-Technologie basiert, sind kaum vorstellbar. ‚Wir hatten Glück, dass wir das überlebt haben.‘ - sagte der Sprecher des estnischen Verteidigungsministers.“

# 7) Alles was recht ist!
## Gesetzliches zum Datenschutz

**Konzerne sind gleich gestellt**

Es gibt kein Konzernprivileg, das zwischen Konzernmutter und Konzerntochter einen freien Datenverkehr möglich macht, weder im österreichischen noch im europäischen Recht. Konzerne sind datenschutzrechtlich weder besser noch schlechter gestellt als Fremdunternehmen. Gemeinsame Datennutzungen innerhalb eines Konzerns sind ein so genannter „Informationsverbund" (siehe Kapitel 2.5.5) und müssen sich genauso an das DSG halten, wie Einzelunternehmen oder Privatpersonen.

## 7.1 Gesetzliche Grundlagen

Für den Schutz von MitarbeiterInnen-Daten sind in Österreich hauptsächlich zwei Gesetze relevant. Das Datenschutzgesetz (DSG) und das Arbeitsverfassungsgesetz (ArbVG). Das DSG beinhaltet die Rechte und Pflichten der Auftraggeber, der BetriebsrätInnen und der Einzelnen. Das ArbVG legt die Mitspracherechte der BetriebsrätInnen fest. Das DSG ersetzt das ArbVG nicht. Der/die Betriebsrat/rätin muss sich mittels beider Gesetze gegen den Missbrauch von MitarbeiterInnen-Daten einsetzen. Die Datenschutzkommission nimmt ihm/ihr die Arbeit der Zustimmung zu Datentransfers nicht ab. Sie kann höchstens unterstützen oder ergänzen.

### 7.1.1 Das Datenschutzgesetz (DSG)

In den vorhergehenden Kapiteln ist bereits einiges zum österreichischen Datenschutzgesetz enthalten. Daher beschränkt sich das Kapitel auf eine knappe Beschreibungen der Gesetzesmaterie.

**Entwicklung**

Erstmals ist 1980 ein Gesetz zum Schutz personenbezogener Daten in Österreich in Kraft getreten. 2000 wurde das Gesetz reformiert und an die Anforderungen der EU-Datenschutzrichtlinie (DSRL) angepasst. Das DSG stand schon immer im Verfassungsrang.

**Grundsätze der Datenverwendung**

Für eine Datenverarbeitung egal ob im In- oder Ausland muss immer klar sein:
- welche Daten,
- aus welcher Quelle,
- zu welchem Zweck,
- wohin übermittelt/überlassen werden,
- bis wann sie aufbewahrt werden und
- wer Zugriff hat.

Außerdem müssen die Betroffenenrechte auf Information, Auskunft, Berichtigung, Löschung und Widerspruch garantiert sein (siehe Kapitel 3).

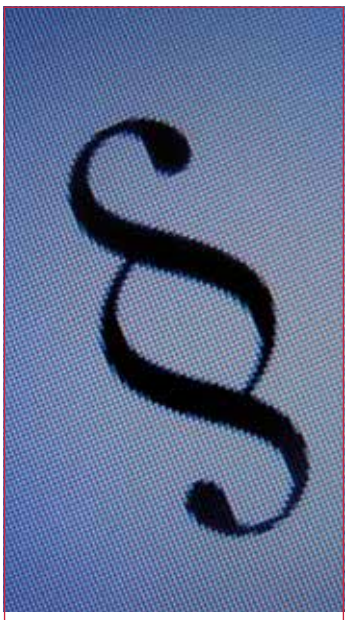
**Grundsätze des Datentransfers**

Grundvoraussetzung für eine gesetzeskonforme **Datenübermittlung oder -überlassung ins Ausland** ist, dass die Daten auch im Inland korrekt erhoben, gespeichert, etc. werden (§ 7 DSG). Das österreichische Datenschutzrecht muss für die Übermittlung von Daten ins Ausland in jedem Fall eingehalten werden. Der Auftraggeber muss vor der Übermittlung oder Überlassung von Daten in das Nicht-EU-Ausland eine Genehmigung der Datenschutzkommission (DSK) einholen (§ 13 DSG) - außer der Datenverkehr mit dem Ausland ist genehmigungsfrei (siehe dazu auch Kapitel 4).

**genehmigungsfreier Datentransfer**

**Genehmigungsfrei** ist der Datenverkehr (§ 12 DSG)[3]:
- an Empfänger von Mitgliedstaaten der EU;

[3] Diese Ausnahmeregelungen des DSG sind weitgehend mit jenen der Datenschutzrichtlinie der EU ident (DSRL Art. 26).



- in Drittstaaten mit angemessenem Datenschutz (welche Drittstaaten angemessenen Datenschutz gewährleisten wird von der EU verordnet und durch Verordnung des Bundeskanzlers national festgelegt. Derzeit sind das: Norwegen, Island, Liechtenstein, Schweiz, Argentinien, Kanada und die beiden Kanalinseln Isle of Man und Guernsey);
- wenn die Übermittlung ins Ausland rechtlich vorgeschrieben ist;
- wenn die Daten im Inland zulässigerweise veröffentlicht wurden;
- wenn die Daten anonym sind;
- wenn die Daten aus Datenanwendungen für private Zwecke oder für publizistische Tätigkeit übermittelt werden;
- wenn eine vertragliche Verpflichtung besteht, die Daten zu übermitteln; der Vertrag muss zwar belegen, dass die Daten mit einem guten Datenschutzniveau übermittelt werden, dennoch ist diese Bestimmung als „Gummiparagraph" zu bewerten;
- wenn eine Zustimmung der Betroffen vorliegt;
- wenn das lebenswichtige Interesse einer Person an der Übermittlung besteht;
- wenn ein wichtiges öffentliches Interesse an der Übermittlung besteht (z.B. Steuerfahndung, Geldwäsche,...) - ein einfaches öffentliches Interesse ist nicht ausreichend.

Außerdem hat die EU-Kommission drei Entscheidungen getroffen, nach denen Daten genehmigungsfrei ins Ausland gebracht werden können:

1. In der **Safe-Harbor-Richtlinie** sind Grundsätze des Datenschutzes festgelegt, denen sich US-Unternehmen freiwillig unterwerfen können, damit die ausreichende Gewährleistung eines angemessenen Datenschutzniveaus anerkannt wird (siehe Kapitel 7.2.1).
2. **Standardvertragsklauseln** ermöglichen eine Datenübermittlung an Auftraggeber in Drittländer ohne angemessenes Schutzniveau, wenn die entsprechenden Vertragsklauseln zwischen den VertragspartnerInnen vereinbart werden. Anstelle der Genehmigungspflicht tritt die Pflicht zur Anzeige an die DSK (§ 13 Abs. 7 DSG) (siehe Kapitel 7.2.1).
3. Nach der Entscheidung über die **Angemessenheit des Datenschutzniveaus** in Kanada und Argentinien zählen diese Länder nunmehr auch zu den Drittländern, in die ein Datenexport ohne Genehmigung vorgenommen werden kann.

**Sanktionen im EU-Vergleich**

Im europäischen Vergleich sind die Sanktionen für Vergehen gegen das DSG relativ gering. Die Kontrollbehörde (die Datenschutzkommission) hat wenig Sanktionsmöglichkeiten. Ein tschechisches Unternehmen wurde beispielsweise gestraft, weil es der Kontrollbehörde den Zugang zu den Daten verweigert hat. In Österreich sind für diesen Fall keine Sanktionen vorgesehen. Die ARGE-Daten merkt zur **Praxis österreichischer Gerichte** bei der Verurteilung von Delikten nach dem DSG an, dass Unternehmen beim ersten Vergehen kaum gestraft werden. Üblicher Weise wird beim ersten mal nur abgemahnt, beim zweiten Mal eine geringe Strafe verhängt beim dritten Mal eine etwas höhere Strafe.

**Sanktionen in Österreich**

Strafen von bis zu **EUR 25.000,-** können verhängt werden, wenn jemand gegen das DSG verstößt (§52 DSG). Wenn zum Beispiel eine verpflichtende Löschung oder Berichtigung nicht durchgeführt wird, wenn jemand sich selbst oder anderen vorsätzlich und widerrechtlich Zugang zu persönlichen Daten verschafft oder auch wenn das Datengeheimnis verletzt wird, dann zieht das eine Geldstrafe nach sich.

Bei **Unterlassungen** zum DSG können Strafen von bis zu **EUR 10.000,-** verhängt werden. Wenn also zum Beispiel die Meldepflicht an die DSK nicht erfüllt und die Genehmigung zum Datentransfer ins Ausland nicht eingeholt wird, wenn Informationspflichten verletzt oder wenn Datensicherheitsmaßnahmen grob außer Acht gelassen werden, dann kann der/die Verantwortliche mit bis zu 9.495 EUR bestraft werden.

Zu Datenanwendung in **Gewinn- und Schädigungsabsicht** beträgt das Strafausmaß maximal ein Jahr Freiheitsstrafe (§ 51 DSG).

Werden Daten gegen einen Betroffenen schuldhaft verwendet, steht dem/der Betroffenen **Schadensersatz** zu (§ 33 DSG). Höhe ist im DSG keine festgesetzt.

**Auswirkungen von Datenmissbrauch auf Führungskräfte**

Man muss den Personen, die Datenverwendungen beauftragen, bewusst machen, dass sie persönlich belangt werden können, wenn sie dem DSG zuwiderhandeln! „Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der Grundsätze, dies gilt auch dann, wenn er für die Datenanwendung Dienstleister hinzuzieht." (§ 6 Abs. 2 DSG). BetriebsrätInnen sollten die Führungskräfte auf diese Straftatbestände hinweisen. Vielleicht wecken sie so mehr Interesse an Lösungen im Sinne der gesamten Belegschaft. Verschafft sich beispielsweise eine Führungskraft ohne Zustimmung der Betroffenen und ohne Legitimation durch eine Betriebsvereinbarung Zutritt zu sensiblen Daten von MitarbeiterInnen, kann sich das in einer Geldstrafe von bis zu 18.890 EUR auswirken. Wird beispielsweise eine meldepflichtige Datenübertragung ins Ausland nicht an die DSK gemeldet, kann der/die ManagerIn persönlich in die Haftung genommen und mit einer Verwaltungsstrafe von bis zu 9.495 EUR belegt werden.

**generelle Geltung des Gesetzes**

Innerbetriebliche Abkommen und Vereinbarungen können niemals das DSG außer Kraft setzen! Die Geheinhaltungsinteressen, die Verschwiegenheitspflicht, Informationsrechte etc. können nicht durch privatrechtliche Verträge aufgehoben werden!

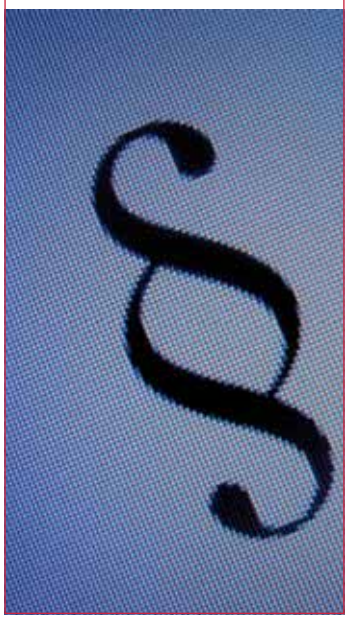
**Beispiel aus der Praxis**
Im Privacy Statement eines Konzerns steht: „Es wird in beiderseitigem Einverständnis auf die Einhaltung des DSG 2000 verzichtet und es gelten nur die individuell vereinbarten Datenschutzregeln." Eine solche Formulierung ist ungesetzlich!

### 7.1.2 Das Arbeitsverfassungsrecht

In den §§ 96 und 96a des Arbeitsverfassungsgesetzes (ArbVG) ist festgelegt, dass bei bestimmten innerbetrieblichen Maßnahmen eine Betriebsvereinbarung zwingend erforderlich ist. In dieser Broschüre sind ausschließlich jene Maßnahmen angeführt, die für den Transfer von MitarbeiterInnen-Daten relevant sind.

**verpflichtende Mitbestimmung des Betriebsrates**

Bezüglich MitarbeiterInnendaten ist beispielsweise die Einführung von **Personalfragebögen**, die mehr als die Stammdaten, Qualifikation und Verwendungsgruppe beinhalten, zustimmungspflichtig. Der Oberste Gerichtshof (OGH) beschreibt diese Personalfragebögen so: „(sie verschaffen) dem/der ArbeitgeberIn Informationen über persönliche Umstände oder Meinungen der einzelnen ArbeitnehmerInnen, an deren Geheimhaltung diese ein Interesse haben könnten." Geht es in einem konkreten Modell lediglich um dienstliche Belange (z.B. Teamfähigkeit, Eloquenz, zielorientiertes Arbeiten, etc.) und nicht auch um persönliche Einstellung und Meinungen, dann wird eher kein Personalfragebogen vorliegen.



Ebenso ist die Einführung von **technischen Systemen zur Kontrolle, sofern diese die Menschenwürde berühren** mitbestimmungspflichtig. Dabei sind die Art der Kontrolle (ob durch Menschen oder durch Technik), die zeitliche Dauer (Stichproben oder permanente Kontrolle), der Umfang der Kontrolle (Verknüpfung verschiedener Daten) und die dabei erfassten Datenarten (Sensibilität!) ausschlaggebend. Gute Beispiele sind hier Arbeitsplätze, die permanent durch eine Kamera überwacht werden - das berührt mit Sicherheit die Menschenwürde.

**Beispiel aus der juristischen Praxis**
Der OGH sieht die Menschenwürde dann berührt, wenn sich jemand ganz individuell kontrolliert fühlt. Der OGH urteilt in Zusammenhang mit der Erfassung von Telefondaten: „Eine Beurteilung der Menschenwürde und ihrer Integrität könne begrifflicherweise an der Sicht der betroffenen Menschen nicht vorbeigehen. Der subjektive Eindruck der Betroffenen von Kontrollsystemen sei daher sehr wohl eines der Kriterien zur Beurteilung der Zustimmungspflichtigkeit." (OGH, Urteil vom 13.6.2002, 8 Ob A 288/01p nach TKG § 88 (alt), ArbVG § 96, MRK Art 8 und StGG Art 10a).
Es reicht laut OGH aus, wenn die objektive Fähigkeit des Systems zur Überwachung gegeben ist, um die Menschenwürde zu berühren - das System muss also nicht tatsächlich zur ununterbrochenen Überwachung eingesetzt werden.


Personalfragebögen und technische Kontrollsysteme, die die Menschenwürde berühren, benötigen also per Gesetz eine Betriebsvereinbarung. Personalfragebögen werden heutzutage in der Regel elektronisch erfasst und ausgewertet, weshalb die Bestimmungen für Datenschutz von MitarbeiterInnendaten zum Tragen kommen. Technische Systeme zur Kontrolle der ArbeitnehmerInnen sind ebenfalls für den Datenschutz von Bedeutung, weil viele der dort erfassten Daten (z.B. Zeitaufzeichnung, Mitarbeitergespräch, etc.) vom Datentransfer betroffen sind.

**Diese Zustimmung des Betriebsrates ist nicht durch Entscheidung der Schlichtungsstelle ersetzbar.**

**ersetzbare Zustimmung des Betriebsrates**

Ersetzbar ist die Zustimmung des Betriebsrates nach § 96a ArbVG, wo es um die Personalbeurteilung und die „Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers" geht.

Bei der **Personalbeurteilung** handelt es sich aber nicht um allgemeine Angaben zur Person und fachliche Voraussetzungen, sondern um darüber hinausgehende Daten. Im Wesentlichen kommt es darauf an, dass im Rahmen dieser Bewertung auch solche Daten erhoben werden, die durch die betriebliche Verwendung nicht gerechtfertigt sind. Solche Daten können insbesondere alle planmäßig nach bestimmten Kriterien geordneten Bewertungen sein (z.B. Flexibilität, Zuverlässigkeit, Risikobereitschaft, Initiative, Führungsverhalten, Kommunikation, usw.).

In der Beurteilung, wann solche Eigenschaften ohne Betriebsvereinbarung bewertet werden dürfen und wann nicht, kommt es auch auf die jeweilige Tätigkeit an (bei einer Führungskraft wird man beispielsweise das Führungsverhalten sehr wohl bewerten dürfen, bei Personen, die überhaupt nicht in die Situation kommen, andere zu führen, wird diese Eigenschaft nicht abgefragt werden dürfen). Die Judikatur legt die Ausnahmebestimmung "durch die betriebliche Verwendung gedeckt" eher eng aus. Hier wird man also sehr schnell zu einer betriebsvereinbarungpflichtigen Maßnahme kommen, dies insbesondere dann, wenn die Beurteilungskriterien schwer messbar (z.B. sehr subjektiv) sind oder sich schwerwiegende Konsequenzen an die Beurteilung knüpfen.

Was die Systeme zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der ArbeitnehmerInnen betrifft, werden darunter in der Regel **Personalverwaltungsprogramme** fallen (z.B. Arbeitszeiterfassung, Telefonanlagen, elektronische Kommunikation und Medien, etc.).

Keine Zustimmungspflicht des Betriebsrates ist dort gegeben, wo bloß allgemeine Daten zur Person und fachliche Voraussetzungen erhoben werden bzw. wenn die tatsächliche oder vorgesehene Verwendung dieser Daten nicht über die Erfüllung von Verpflichtungen hinaus geht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben. In der Regel werden in Personalverwaltungssystemen aber auch noch darüber hinausgehende Daten gespeichert und verarbeitet.

**die Schlichtungsstelle**

Wird keine Einigung zwischen Geschäftsführung und Betriebsrat mittels Betriebsvereinbarung erzielt, kann die Schlichtungsstelle angerufen werden (§ 96a Abs. 2 ArbVG). Fehlt eine Betriebsvereinbarung bzw. hat die Schlichtungsstelle nicht entschieden, so darf die jeweilige Datenverarbeitung gar nicht erst eingesetzt werden. Es gibt hier auch Unterlassungs- bzw. Beseitigungansprüche des Betriebsrates. Die Entscheidung der Schlichtungsstelle steht allerdings über der Meinung der ArbeitgeberInnen bzw. der ArbeitnehmerInnenvertretung. Die Anrufung der Schlichtungsstelle kann auch einen unerwünschten Ausgang haben, der dann aber akzeptiert werden muss.

**Parteistellung im Datenschutzgesetz**

Anders als im ArbVG, wo der Betriebsrat auf die Einhaltung der Betriebsvereinbarung klagen kann, hat der Betriebsrat aber nach dem DSG keine Klage zur Verletzung des DSG einreichen. Der Betriebsrat hat keine eigene Position vor Gericht, wenn MitarbeiterInnen gegen das DSG vorgehen wollen. Sie können MitarbeiterInnen vor Gericht nicht vertreten. (JusristInnen nennen das: Betriebsräte haben keine Parteistellung.)

**Zustimmung von Betriebsrat und MitarbeiterInnen**

In Österreich besteht somit die besondere Situation, dass Datentransfers von personenbezogenen Daten sowohl nach dem DSG als auch nach dem ArbVG beurteilt werden müssen. Wenn es sich also um Daten handelt, die beispielsweise sowohl nach dem DSG unter sensible Daten fallen als auch nach § 96 ArbVG eine Zustimmung seitens des Betriebsrates erfordern, kann man nicht das Eine durch das Andere ersetzten. Es geht nicht, dass man sich z.B. für den Transfer von Gesundheitsdaten, die in Personalfragebögen erfasst werden sollen, ausschließlich die Zustimmung der Betroffenen einholt, den Betriebsrat aber nicht mitbestimmen lässt. Es geht auch nicht, dass man nur den Betriebsrat fragt, ob biometrische Daten für automatische Kontrollsysteme verwendet werden dürfen (z.B. Zeiterfassungssysteme) und die Betroffenen aber nicht um ihre Zustimmung bittet.

**Beim Transfer von bestimmten sensiblen Daten müssen sowohl Betroffene als auch Betriebsrat zustimmen!**

**Information des Betriebsrates**

Nach § 91 DSG ist der Arbeitgeber verpflichtet, den Betriebsrat über bestimmte Vorgänge im Betrieb zu informieren. Dazu zählt auch die Informationspflicht darüber „welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht." (§ 91 Abs. 2 DSG).

## 7.2 Ergänzende Gesetze

Zusätzlich zu diesen zwei Hauptwerken werden je nach Sachlage noch andere Gesetzesmaterien wichtig. Diese sind hier nur in aller Kürze, geordnet nach ihrer Priorität im Stufenbau der österreichischen Rechtsordnung angeführt, um die Komplexität des Themas anzudeuten. Falls es die Sachlage erfordert, muss in den jeweiligen Werken nachgesehen werden.

### 7.2.1 Datenschutz-Richtlinie der EU (DSRL)

**Ziel der EU-Richtlinie**

Die Datenschutz-Richtlinie der EU (DSRL) wurde 1995 mit dem Ziel erlassen, den freien Datenverkehr zu ermöglichen. Die EU hat beschlossen, dass mit der Umsetzung der Richtlinie in nationales Recht **alle Staaten innerhalb der EU-Grenzen ein angemessenes Schutzniveau** für personenbezogenen Daten haben und daher der Transfer in alle EU-Staaten weitgehend unbegrenzt möglich ist. Die Freiheit des Güter- und Personenverkehrs wurde damit auch auf die Freiheit des Datenverkehrs ausgedehnt. Was genau „angemessen" ist, entscheidet die EU. In Länder ohne angemessenes Schutzniveau ist der Datentransfer personenbezogener nicht erlaubt. In Österreich genehmigt die DSK den allfälligen Datentransfer in Drittstaaten ohne angemessenes Schutzniveau.

**angemessenes Schutzniveau**

Die Datenschutzrichtlinie der EU (DSRL) bietet einen Mindeststandard an Datenschutz, der in allen Mitgliedsländern in nationales Recht umgesetzt werden muss. Die DSRL ist also die Grundlage für die nationalen Datenschutzgesetzgebungen. EWR-Länder bieten per

EU-Entschluss ebenfalls ein angemessenes Schutzniveau wodurch der Datentransfer prinzipiell zulässig ist: **Island, Liechtenstein und Norwegen**. Auch die Drittstaaten **Argentinien, Kanada, Schweiz, Israel** sowie die **Insel Guernsey** (ein „Steuerparadies" unter den Kanalinseln) und die **Isle of Man** haben ein angemessenes Datenschutzniveau. Betrachtet man das Schweizer Datenschutzgesetz aus dem Jahre 1992, kann man allerdings keinen hochwertigen Datenschutz feststellen. Es fehlen beispielsweise die Informationspflicht gegenüber den Betroffenen und die Bewilligungspflicht durch Kontrollbehörden. Dennoch zählt die Schweiz zu den Ländern mit angemessenem Schutzniveau. Derzeit wird das Schweizer Gesetz überarbeitet.

**Einhaltung nationaler Datenschutzbestimmungen**

Egal, wo der Konzern seine Zentrale hat, die europäische DSRL bestimmt, dass das nationale Recht zu gelten hat, je nachdem wo sich die **Niederlassungen** des Konzerns befinden. Eine Niederlassung ist dann gegeben, wenn eine feste Einrichtung besteht wo die Firma tatsächlich tätig ist - die jeweilige Rechtsform ist dabei ebenso egal wie die Gewinnabsicht. Auch der Flugschalter einer Airline, ein gemeinnütziger Verein oder das Baustellenbüro eines Hoch- und Tiefbauunternehmens gelten als Niederlassung.

**Sanktionen**

Selbst wenn der Konzern nur die Mittel in einem EU-Mitgliedsstaat nutzt, ist das jeweilige nationale Datenschutzrecht einzuhalten. Der Begriff der **„Nutzung von Mitteln"** (Art. 4 DSRL) wird allerdings unterschiedlich interpretiert.

Die DSRL lässt einigen Interpretationsspielraum auf nationaler Ebene. Das zeigt sich besonders bei den Sanktionen, wo es heißt „Die Mitgliedsstaaten ergreifen geeignete Maßnahmen (…) und legen die Sanktionen fest …" (Art. 24 DSRL). Das reicht dann von keinen festgelegten Strafen in Estland, Lettland und Litauen bis hin zu einer Million Euro in Griechenland.

## Standardvertragsklauseln

**Zielsetzung**

Zur Erfüllung von Verträgen mit Nicht-EU-Staaten gibt es die Möglichkeit zwischen den Vertragspartnern so genannte „Standardvertragsklauseln" zu beschließen. Länder mit angemessenem Schutzniveau können an Länder ohne angemessenes Schutzniveau Daten übermitteln, wenn sie die Standardvertragsklauseln anwenden. Diese Klauseln sollen vertraglich absichern, dass Daten nicht missbräuchlich verwendet werden können, selbst wenn in dem Land der Datenverarbeitung generell keine gutes gesetzliches Datenschutzniveau vorhanden ist.

Ein österreichisches Unternehmen kann also zum Beispiel mit Standardvertragsklauseln seine Daten ohne weiteres zur Personalverrechnung nach Indien übermitteln, obwohl in Indien generell kein angemessenes Datenschutzniveau besteht.

**Geschichte**

Die Standardvertragsklauseln wurden von vielen Drittstaaten als wettbewerbsverzerrend hart kritisiert. Insbesondere die USA sahen sich durch die EU-internen Erleichterungen im internationalen Datenverkehr benachteiligt. Nach dreijährigen Verhandlungen zwischen der Internationalen Handelskammer, der EU-Kommission und der dem Ausschuss der EU-Datenschutzaufsichtsbehörden (der so genannten „Artikel-29-Datenschutzgruppe") wurden im Dezember 2004 neue Standardvertragsklauseln beschlossen. Sie gelten als „unternehmensfreundlicher". Davon erhofft man sich eine häufigere Nutzung der Standardvertragsklauseln.

**Haftung in den neuen Klauseln**

Die ARGE Daten beurteilt die neuen Klauseln: „Eine sehr wichtige Änderung ist bezüglich der Haftung vorgesehen: Während in den 'alten' Klauseln eine gesamtschuldnerische Haftung vorgesehen war, die viele Unternehmen von der Benützung der Klauseln abhielt, ist nun ein abgestuftes Haftungssystem vorgesehen, in dem jeder Vertragspartner für die von ihm verursachten Schäden haftet. Dasjenige Unternehmen, das Daten übermittelt, haftet allerdings auch für ein eventuelles Auswahlverschulden im Bezug auf den Übermittlungsempfänger." 2008 wird die nächste Überprüfung statt finden.

**Beschränkung des Datentransfers**

Bei den Standardvertragsklauseln besteht immer die Beschränkung, dass die Daten einzig und allein für den **Zweck der Vertragserfüllung** verwendet werden dürfen. Ausschließlich das, was für den Vertrag wesentlich ist, darf also an Daten übermittelt werden.

**Genehmigungspflicht**

Standardvertragsklauseln müssen von der DSK genehmigt werden! Das hat seine Ursache darin, dass personenbezogene Daten in Dritt-Staaten übermittelt werden sollen (siehe Kapitel 4.2). Die Verwendung von Standardvertragsklauseln erleichtert das Genehmigungsverfahren bei der DSK erheblich. Nur in seltenen Fällen, verweigert die DSK den Datentransfer mittels Standardvertragsklauseln.

**Aus dem Bericht der Datenschutzkommission 2007**

In einem Konzern sollte Daten zwischen der Zweigniederlassung in Österreich und der us-amerikanischen Muttergesellschaft übermittelt werden. Dem Antrag waren Standardvertragsklauseln beigelegt in denen der Zweck "...for worldwide statistic reports and editing"[4] angegeben war. Die DSK forderte eine Nachbesserung. Die Antragstellerin erklärte, dass kein „editing" in den USA stattfinden würde. Die DSK hielt diese Erklärung für nicht ausreichend, weil die vertragliche Basis der Übermittlung der Daten ins Ausland dem Datenimporteur eine erheblich andere Datenverwendung erlauben würde als die vom Exporteur beantragte Genehmigung. Daher sei eine in der Genehmigung eingeschränkte Verwendung im Ausland schwer durchsetzbar. Weiters hob die DSK hervor, dass angesichts der speziellen Organisationsstruktur eines Konzerns die Rechtsdurchsetzung des österreichischen Exporteurs gegenüber dem Datenimporteur, der ihm im Konzern übergeordnet und weisungsberechtigt ist, realistischerweise keine aussichtsreiche Perspektive eröffnet. Weiters hielt die DSK die Übermittlung wegen des Umfangs der betroffenen Personaldaten als auch hinsichtlich des Eingriffspotentials für gravierend.
(Bescheid IDVK GZ: K178.231/0007-DSK/2007 vom 21.03.2007)

**Inhalt des Vertrags**

Die Standardvertragsklauseln sind ein von der EU-Kommission vorgefertigtes Formular, in das die Vertragsparteien nur noch ihre Unternehmensdaten sowie die Einzelheiten der konkreten Daten-Übermittlung eintragen müssen. (Ein Link im Anhang verweist auf das Formular der EU-Kommission zu den Standardvertragsklauseln.)

In dem Vertrag verpflichtet sich der Datenexporteur die Daten rechtmäßig zu verwenden sowie dazu, Anfragen der Datenschutzkommission und der betroffenen Personen zu beantworten. Der Datenimporteur willigt ein, Fragen des Datenexporteurs jederzeit zu beantworten und seine Verfahren der Datenverarbeitung durch den Exporteur prüfen zu lassen.[5]

**Parteistellung vor Gericht**

Der Vorteil der Standardvertragsklauseln für **ArbeitnehmerInnen** ist, dass sie **direkt klagen** können, sollte ihm/ihr ein persönlicher Schaden entstanden sein. Das Gerichtsverfahren muss dann im Inland - dort wo der Betroffene Klage eingereicht hat - abgewickelt werden. Die Betroffenen sind hier also besser dran, als nur mit der DSRL, die kein Recht auf Einzelklagen gewährt.

## Safe-Harbor-Richtlinien

**Entstehungsgeschichte**

Die USA als ein wichtiger Handelspartner der EU war weder über die Datenschutzrichtlinie noch über die Standardvertragsklauseln erfreut. Dort herrschen andere Maßstäbe im Datenschutz. Erst nach zähen Verhandlungen zwischen dem Handelsministerium der USA und der EU hat man sich zu einem datenschutzrechtliche „sicheren Hafen", den „Safe-Harbor-Bestimmungen", durchgerungen.

[4] Auf Deutsch: „.. für weltweite statistische Berichte und Datenaufbereitung".
[5] Ähnlich den allgemeinen Standardvertragsklauseln gibt es auch solche, die für Dienstleister - und nicht Vertragspartner - in Drittstaaten ohne angemessenes Datenschutzniveau angewandt werden können; die so genannten „Auftragsverabeiter-Standardvertragsklauseln".

In dem Abkommen können sich einzelne Firmen freiwillig verpflichten, Datenschutzbestimmungen zu befolgen, die an die EU-Richtlinie angepasst wurden. Es gibt verschiedene Arten von Mitgliedschaften bei Safe-Harbor, je nachdem welche Daten der Firma den Bestimmungen unterliegen (z.B. ausschließlich KundInnendaten, Daten von Handelspartnern, MitarbeiterInnen-Daten). Deshalb sollte man bei der Überprüfung ob ein Unternehmen Safe-Harbor zugestimmt hat oder nicht auf jeden Fall auch nachschauen, für welche Daten die Safe-Harbor-Bestimmungen gelten!

**Sonderfall USA**

Im Oktober 2007 waren in etwa 1.200 Unternehmen in die Liste eingetragen und haben somit den Safe-Harbor-Richtlinien akzeptiert. Das Handelsministerium überprüft die Datenschutzbestimmungen der Firmen. Die Mitgliedschaft bei Safe-Harbor muss jährlich erneuert werden.

Auch Safe-Harbor ermöglicht es den Betroffenen auf Verletzung der Richtlinie zu **klagen** - allerdings haben die Betroffenen nicht das Recht auf ein Gerichtsverfahren im Inland. Die Klage muss nach dem jeweiligen nationalen Recht des/der Klägers/-in durchgeführt werden. Das bedeutet in der Regel, dass Unternehmen in den USA nicht belangt werden.

**Sanktionen**

### 7.2.2 Europäische Menschenrechtskonvention (EMRK)

Die EMRK Artikel 8 beinhaltet das **Recht auf Achtung des Privat- und Familienlebens**. Insbesondere staatliche Eingriffe in dieses Menschenrecht sind „unstatthaft". Daraus wird abgeleitet, dass persönliche Daten besonders schützenswürdig sind und nicht einfach weiter gegeben werden können. Insbesondere öffentliche Stellen müssen das Privat- und Familienleben schützen und dürfen nur im Notfall eingreifen.

**Achtung des Privat- und Familienlebens**

### 7.2.3 Staatsgrundgesetz (StGG)

Die Rechte der StaatsbürgerInnen sind im StGG festgehalten. Dazu zählt das Briefgeheimnis (art. 10 StGG), das Fernmeldegeheimnis (Art. 10a StGG) und die Pressefreiheit (Art 13 StGG).

### 7.2.4 Verfassungsgerichtshof (VfGH)

Einige Entschiede des VfGH legen Persönlichkeitsrechte des/der Einzelnen fest, die auch für den Datenschutz relevant sind. Das Recht auf Achtung des Privat- und Familienlebens wird darin festgelegt.

### 7.2.5 Strafgesetzbuch (StGB)

Aus dem StGB wurden hier jene Gesetzesmaterien zusammengefasst die im Zusammenhang mit Datenschutz relevant werden können.

Eine Freiheitsstrafe bis zu sechs Monaten oder eine Geldstrafe von bis zu 360 Tagessätzen handelt sich ein, wer **Daten, die nicht für ihn/sie bestimmt sind selbst benutzt** (§ 118a StGB nennt das „widerrechtlicher Zugriff auf ein Computersystem").

**Computerkriminalität**

Auch wer diese Daten anderen, für die sie ebenfalls nicht bestimmt sind, zur Verfügung stellt oder sie sogar **öffentlich macht**, kann diese Strafe erhalten. Auch das missbräuchliche Abfangen von Daten kann mit demselben Strafausmaß verfolgt werden (§ 119a StGB).

Außerdem kennt das Strafgesetzbuch für **Datenbeschädigung** ein Strafausmaß von Freiheitsstrafen bis zu fünf Jahren oder 50.000 EUR Geldstrafe (§ 126a StGB). Bei diesen Vergehen handelt es sich vorwiegend um Computerkriminalität, Datenanwendung in Gewinn- und Schädigungsabsicht.

Der **Missbrauch von Computerprogrammen oder Zugangsdaten** kann mit einer Freiheitsstrafe von einem halben Jahr bzw. den entsprechenden Tagsätzen Geldstrafe belegt werden (§ 126c StGB).

Bei **Bereicherung**(-sabsicht) für sich selbst oder Dritte bzw. **betrügerischem Datenverarbeitungsmissbrauch** (§ 148a StGB) kann sogar - je nach Schadenshöhe - bis zu zehn Jahren Freiheitsstrafe verhängt werden.

**persönliche Verantwortung**

**Strafrechtlich ist immer die durchführende Person verantwortlich.** Das Unternehmen haftet im Strafrecht nicht für seine Angestellten. Eine Weisung durch den/die Vorgesetzte entbindet die Angestellten aber nicht von ihrer strafrechtlichen Verfolgung - vielleicht wird eine solche Weisung als strafmildernd anerkannt. Falls jedoch eine strafrechtswidrige Weisung auf ihrem Schreibtisch landet, weisen sie sie lieber zurück, besprechen sie sich mit dem Betriebsrat und/oder wenden sie sich an ihre Interessenvertretung!

### 7.2.6 Unternehmensstrafrecht (VbVG)

**unternehmerische Verantwortung**

Seit 2006 können auch Unternehmen bzw. Verbände strafrechtlich belangt werden - mit dem Verbandsverantwortlichkeitsgesetz (VbVG). Bis dahin war dies nur bei individuellen Personen möglich, die sich bei ihrer Arbeit gesetzeswidrig verhalten haben. Unternehmen haften nun für rechtswidrige und schuldhafte Handlungen ihrer MitarbeiterInnen. Damit wird die zunehmende Komplexität von Unternehmensstrukturen nun auch im österreichischen Recht berücksichtigt.

### 7.2.7 Telekommunikationsgesetz (TKG)

**Geltungsbereich**

**Inhalt**

Betroffen vom TKG sind ausschließlich BenutzerInnen und Dienstleister/Betreiber/Anbieter/Bereitsteller von Kommunikationsnetzen und/oder Kommunikationsdiensten, kurzum Firmen aus dem IKT-Bereich. Das TKG befasst sich in Zusammenhang mit Datenschutz vorwiegend mit der Verwendung von KundInnen- und KonsumentInnen-Daten. Diese müssen in die Verwendung ihrer Daten zu Werbezwecken immer einwilligen (§ 107 TKG). 2002 hat die EU eine Richtlinie zur elektronischen Kommunikation erlassen (Richtlinie 2002/58/EG).

### 7.2.8 Sicherheitspolizeigesetz (SPO)

Die **Sicherheitsbehörden** dürfen personenbezogene Daten ermitteln und weiterverarbeiten. Die Bedingungen unter denen das zulässig ist, sind genau geregelt (§ 53 SPO).

### 7.2.9 Mediengesetz (MedienG)

**immaterieller Schaden**

Werden sensible Daten so verwendet, dass die **Kreditwürdigkeit** einer Person oder ihre **Geheimhaltungsinteressen geschädigt** werden, kommt das Mediengesetz zum Tragen (§7 Abs. 1 MedienG). Für die erlittene Kränkung durch die Veröffentlichung kann eine Strafe von bis zu 20.000 EUR auferlegt werden. Das DSG kennt zwar diesen immateriellen Schaden auch (§ 33 DSG), nennt aber keine Strafausmaße dafür. Nach dem DSG handelt es sich bereits um eine strafbare Tat, wenn die Daten zwar nicht veröffentlicht, aber die schutzwürdigen Geheimhaltungsinteressen so verletzt wurden, dass eine Person „im Sinne des § 7 MedienG" bloß gestellt wird.

### 7.2.10 E-Governmentgesetz (E-GovG)

**Datenanwendung durch den Staat**

Bis zu 20.000 EUR Geldstrafe können verhängt werden, wenn **Stammdaten nicht im Sinne des Gesetzgebers verwendet** werden (§ 22 E-GovG). Es ist also strafbar, Stammdaten oder bereichsbezogene Personenkennzeichen (darunter versteht man beispielsweise Kundennummern) zu ermitteln um damit weitere personenbezogene Daten

der Betroffenen heraus zu bekommen. Unbefugte Speicherung, Benutzung oder zur Verfügung Stellung für Dritte ist ebenfalls verboten.

### 7.2.11 E-Commerce-Gesetz (ECG)

**Datenanwendung durch IKT-Firmen**
(IKT = Informations- u. Kommunikationstechnologie)

Das E-Commerce-Gesetz regelt in den Paragraphen 13 bis 18 die **Verantwortung spezifischer Diensteanbieter** (z.B. Suchmaschinen-Anbieter, Access-Provider, Hosting-Firmen). Unter bestimmten, genau festgelegten Voraussetzungen ist es für spezifische Diensteanbieter nämlich möglich, persönliche Daten - zumindest für einen kurzen Zeitraum - zu speichern, für Dritte zugänglich zu machen und zu übermitteln.

### 7.2.12 Allgemeines Bürgerliches Gesetzbuch (ABGB)

**Haftung**

Die Haftung ist generell eines der komplexesten Themen in der Rechtsprechung. Zur Haftungsfrage klärt das ABGB, dass auch „wer anderen zu einer Leistung verpflichtet ist" (z.B. Beschäftigte) nicht nur **für seine rechtlichen VertreterInnen und deren Verhalten haftet, sondern genauso für das eigenes Verhalten** (§ 1313a ABGB). Die Beweislast für das Schlagendwerden einer Haftung liegt allerdings bei dem/der KlägerIn.

**Sorgfaltspflicht**

Gewerbetreibende unterliegen einem so genannten **„erhöhten Sorgfaltsmaßstab"** (§ 1299 ABGB). Das heißt, der/die Kunde/in kann davon ausgehen, dass der/die Gewerbetreibende die erforderlichen Qualifikationen auch tatsächlich hat. Wer also bei einem Gewerbe einkauft, das elektronische Daten verwendet, kann davon ausgehen, dass sich die Gewerbetreibenden mit dem Datenschutz auskennen.

### 7.2.13 Gewerbeordnung (GewO)

**Werbung teilweise erlaubt**

Hier ist geregelt, dass für **Marketingzwecke** Stammdaten verwendet werde dürfen und dass personenbezogenen Daten (taxativ aufgelistet) auch an Marketingunternehmen weitergegeben werden dürfen - allerdings nur unter der Voraussetzung, dass die Betroffenen darüber **informiert** wurden und die Möglichkeit erhalten haben, diese Datenanwendung zu untersagen (§ 151 GewO). Das **Widerspruchsrecht der Betroffenen** muss also gewahrt bleiben. Der/die Gewerbetreibende muss dabei der Firma, der die Daten übermittelt werden schriftlich versichern, dass die Betroffenen informiert wurden und die Möglichkeit erhalten haben, die Datenübermittlung zu verweigern.

Da es sich hier um eine Kann-Bestimmung handelt, ist es den Gewerbetreibenden freigestellt, Datenweitergabe zu Marketingzwecken auch ganz bleiben zu lassen und dies den KundInnen auch zu kommunizieren - vielleicht ergibt sich ja dadurch ein neuer Wettbewerbsvorteil.

### 7.2.14 Exekutionsordnung (EO)

Die Exekutionsordnung besagt, dass bei **Zuwiderhandeln gegen eine Richterentscheidung** (z.B. Unterlassung der Datenverarbeitung weil diese rechtswidrig ist), Geldstrafen bis zu 100.000 EUR zulässig sind (§ 354, § 359 EO).

# 8) Was tun?
## Handlungs- und Gestaltungsebenen

**Hauptschwierigkeiten beim Datentransfer**

Die häufigsten Probleme, die es zu vermeiden gilt, sind:

- unsystematisches Vorgehen mit Einzellösungen ohne ein nachhaltiges, gut geplantes Konzept;
- ausschließlich technische Lösungsversuche ohne Berücksichtigung organisatorischer Komponenten, aber die beste Software nützt nichts, wenn die MitarbeiterInnen nicht genügend geschult werden um sie auch anzuwenden;
- MitarbeiterInnen werden nicht informiert, sind daher nicht sensibilisiert für das Thema und es unterlaufen Fehler aus Unkenntnis;
- Management macht Lippenbekenntnisse zum Datenschutz ohne die Tragweite des Themas zu erfassen.

**Auswirkungen der Unklarheiten**

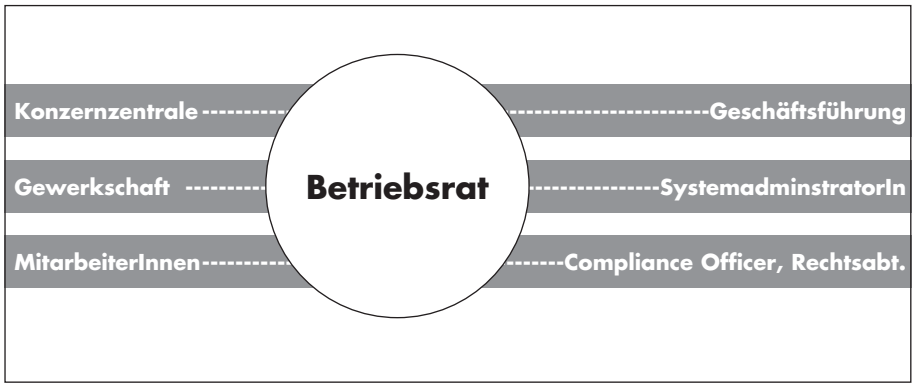
Für kritische Beschäftigte stellen sich zunehmend die Fragen: Wer wird aller davon erfahren, wenn Gespräche aufgezeichnet werden? Wie lange werden Daten für meineN VorgesetzteN einsichtig sein? Inwiefern kann das alles meine Karriere beeinflussen? Soll ich bestimmte Daten bekannt geben oder wird mir das einmal schaden? Die vorbeugende Selbstüberwachung nimmt zu. Die technischen Möglichkeiten und deren Nutzung bei der innerbetrieblichen Überwachung verursachen Druck auf ArbeitnehmerInnen.

Um den innerbetrieblichen Datentransfer transparenter und somit auch beeinflussbarer zu gestalten, sind in diesem Kapitel Möglichkeiten dargestellt, wie diese Ziele erreicht werden können.

## 8.1 Strategien des Betriebsrates

**zentrale Kontrollinstanz**

Neue Systeme, die im Betrieb ausgerollt werden sollen, müssen zuerst dem Betriebsrat vorgelegt werden, ob sie die bestehenden Datenschutzbestimmungen (z.B. Gesetzgebung, interne Verhaltensregeln, etc.) befolgen. Befragungen der MitarbeiterInnen, neue SAP-Bausteine, neue Zeiterfassungssysteme u.s.w. sollen zuerst im Betriebsrat begutachtet werden. Nur sensibilisierten MitarbeiterInnen fällt auf, ob relevante Neuerungen geplant oder sogar schon durchgeführt werden. Nur informierte Betriebsräte wenden sich dann ihrerseits an externe ExpertInnen von der Gewerkschaft um die neuen Systeme überprüfen zu lassen. Der Betriebsrat stellt in jedem Fall die Schnittstelle dar, an der kontrolliert werden sollte, ob die bestehenden Regelungen auch tatsächlich eingehalten werden. **Der Betriebsrat ist der Kreisverkehr, den jede geplante Maßnahme passieren muss.**

**Unsicherheit der Einzelnen >> kollektives Handeln**

Die einzelnen MitarbeiterInnen interessieren sich zwar dafür, welche Daten über sie weitergegeben werden, trauen sich aber oft nicht, Einsicht zu nehmen, Auskunft zu verlangen oder gar Löschungen zu beantragen, weil sie negative Folgen befürchten. Nachdem der Betriebsrat kein Recht hat, allgemeine Personaldaten abzufragen, muss ein individueller **Anlassfall** gegeben sein, damit der/die Betriebsrat/rätin intervenieren kann. Um sich dennoch nicht den Weg als EinzelkämpferIn durchschlagen zu müssen, kann der/die Betriebsrat/rätin eine Sammelabfrage mehrere ArbeitnehmerInnen gemeinsam starten. Der/die Betriebsrat/rätin könnte im Betrieb fragen, wer aller Interesse an einer solchen Abfrage hat. Die Ergebnisse können dann zur Information und Sensibilisierung der gesamten Belegschaft herangezogen werden.

**Betriebsversammlung und Arbeitsgruppen**

Um Unklarheiten im Datenschutz zu vermeiden, kann auch eine Betriebsversammlung zum Thema Datenschutz helfen. Sind dazu auch externe ExpertInnen eingeladen, kann die Belegschaft zusätzlich von deren Wissen profitieren.

Auch **interne Arbeitsgruppen** unterstützen dabei, sich einen Weg durch den „Datendschungel" zu bahnen. Dabei können Sensibilisierungsarbeit geleistet, Lücken aufgedeckt, gemeinsame Vorgehensweisen geplant werden,…

Eine **Forderung an die Geschäftsführung** in diesem Zusammenhang wäre die Erfassung des Status quo in Datenangelegenheiten - am besten unter Einbeziehung der SystemadministratorInnen. Das schafft sicher mehr Klarheit (z.B. welche Datenanwendungen gibt es im Betrieb, wer hat Zugang, welche Daten sind erfasst, …).

**Abgrenzung von Geschäftsbereich und Betrieb**

Die Grundlage für jegliches Handeln des Betriebsrates zum Thema Datenschutz ist die Abgrenzung von Geschäftsbereich und Betrieb. Erst wenn abgeklärt ist, auf welche betriebsinternen Einheiten sich der Datentransfer bezieht, können weitere Schritte erfolgen. Erst nach der exakten Definition von Betrieb und Geschäftsbereich sollte die weitere strategische Vorgehensweisen überlegt werden, denn davon hängt es ab, welche Datentransfers rechtlich zulässig sind und welche nicht. Um die Sachlage mit einem medizinischen Beispiel zu verdeutlichen: Erst wenn die Diagnose gestellt ist, kann eine angemessene Therapie gefunden werden.

**komplexe Unternehmensstrukturen**

Die Abgrenzung zwischen den verschiedenen Betrieben/Unternehmen/Geschäftsbereichen innerhalb eines Konzerns ist in Zeiten der zunehmend komplexen und verflochtenen Firmenstrukturen von ganz wesentlicher Bedeutung - und gehört nicht zu den einfachen Aufgaben. Das DSG behandelt unterschiedliche Geschäftsbereiche wie unterschiedliche Unternehmen. Außerdem ist es wichtig, zu wissen, ob rechtlich gesehen ein anderes Unternehmen vorliegt oder nicht, um zu entscheiden, ob eine Datenübertragung vorliegt oder nicht. Je nachdem gelten nämlich bestimmte Schutzbestimmungen - oder auch nicht. Innerhalb eines Unternehmens dürfen Daten zum selben Zweck durchaus übermittelt werden - vorausgesetzt die Prinzipien für den Datentransfer werden eingehalten (siehe Kapitel 3).

### 8.1.1 Wo beginnt der Geschäftsbereich und wo endet er?

**meldepflichtige Übermittlung von Daten**

Übermittlung von Daten kommt mitunter innerhalb desselben Unternehmens vor. Meldepflichtig ist die Datenübermittlung dann, wenn:

- ein anderer Zweck als der ursprüngliche damit verfolgt wird;
- es sich nicht um eine Standard- oder Musteranwendung (vgl. Kapitel 4.1) handelt und
- die Daten außerhalb eines Geschäftsbereichs verwendet werden.

Der Begriff „Geschäftsbereich" ist allerdings gesetzlich nicht näher definiert. Man kann sich dabei an der innerbetrieblichen Organisation von Aufgaben, Abteilungen und Abläufen orientieren.

**Fiktives Beispiel**
Wenn die Personalabteilung eine Datenbank betreut, die alle Schulungs- und Weiterbildungsmaßnahmen erfasst, um die Administration dieser Kurse zu erleichtern, dürfen die dort gespeicherten Daten nicht einfach an die Personalverrechnung weitergegeben werden, damit diese allfällige Bonusse aus der erreichten Punktezahl bei einer Weiterbildungsmaßnahme berechnet. Die Daten würden dann den Geschäftsbereich „Weiterbildung" verlassen und in einem anderen Geschäftsbereich „Personalverrechnung" verwendet werden.

**Fiktives Beispiel**
Wenn hingegen eine Kundenbestellung von der IT-Abteilung, wo sie per E-Mail eingegangen ist, zur Marketing-Abteilung übermittelt wird, wo die Bestellung administriert wird und von dort weiter zum Verkauf, damit dort die Bestellung abgewickelt wird, handelt es sich um den selben Geschäftsbereich „Kundenservice". Zweck ist die Abwicklung einer Kundenbestellung. Es sind hier zwar mehrere Abteilungen involviert, aber der Zweck und der Bereich sind der selbe - somit besteht keine Meldepflicht.

**Beispiel aus der Finanzwirtschaft**
MitarbeiterInnen erhalten im Rahmen eines Beteiligungsmodells Aktien vom Unternehmen. Das Personalwesen liefert als Grundlage für die Zuteilung eine Liste der anspruchsberechtigten MitarbeiterInnen an den Wertpapierbereich, der die Einbuchung der Aktien auf das jeweilige Mitarbeiter-Depot vornimmt. Die Aktien sind also im Besitz der MitarbeiterInnen. Das Problem bei der Sache ist nun, dass das Personalwesen eine generelle Auswertung der Wertpapierdepots von MitarbeiterInnen vom Wertpapierbereich verlangt, ob und wenn ja, welche MitarbeiterInnen ihre Unternehmensaktien wieder verkauft haben. Der Betriebsrat/die Betriebsrätin begaben sich auf Recherche. Ergebnis: Diese Vorgangsweise entspricht nicht dem ursprünglichen Verwendungszweck (Personalverrechnung) der vom Personalwesen gespeicherten Daten. Typischerweise ist der Wertpapierbereich ein anderer "Geschäftsbereich" (dieser Begriff wird im DSG 2000 zwar nicht definiert, lässt sich jedoch aus verschiedenen gesetzlichen Bestimmungen wie Gewerberecht, Handelsrecht, Vereinsrecht etc. ableiten). Unterschiedliche Geschäftsbereiche sind wie unterschiedliche Unternehmen zu behandeln. Daher ist zu prüfen, ob ein Auftrag seitens der betroffenen MitarbeiterInnen zu dieser Datenübermittlung besteht und ob die Datenübermittlung überhaupt zulässig ist. Eine Zustimmungserklärung des/der MitarbeiterIn für die generelle Datenweitergabe von Wertpapierbereich an Personalwesen liegt nicht vor. Möglich ist eine Datenweitergabe vom Wertpapierbereich an das Personalwesen nur dann, wenn es sich im Einzelfall um versteuerungsrelevante Ereignisse handelt, die in der Lohnverrechnung zu berücksichtigen sind. Es besteht aber keine rechtlich legale Möglichkeit zur generellen Bestandsauswertung, da diese ja auch selbst gekaufte Aktien und auch jene außerhalb der steuerrechtlichen Behaltefrist umfassen würde.

## 8.1.2 Wo beginnt der Betrieb und wo endet er?

**Betriebsbegriff im österreichischen Recht**

Die sechs wesentlichen Merkmale des Betriebes sind (§ 34 ArbVG):

1. Die **organisatorische Einheit**; sie drückt sich in der Einheit des Betriebsinhabers, des Betriebszweckes und der Organisation aus. Es muss ein gewisses Mindestmaß an Selbstständigkeit vorliegen und das Ergebnis des Arbeitsvorganges muss von anderen betrieblichen Vorgängen unabhängig sein. Umgekehrt gesagt: sind einzelne Abteilungen mit völlig unterschiedlicher Selbstständigkeit und in unterschiedlicher Abhängigkeit von der Zentrale ausgestattet und werden unterschiedlichste Aufgabenstellungen verfolgt, kann nicht von einem Betrieb gesprochen werden.
2. Der **Betriebsinhaber**; er/sie ist eine physische oder juristische Person oder eine Personengemeinschaft - wird vom Gesetz nicht näher definiert. An ihn richten sich aber Normen und Sanktionen.

3. Die **Beschäftigten**; sie sind die auf Dauer berechnete Vereinigung von Arbeitskräften zur Erzielung bestimmte Betriebsergebnisse. Ein Betrieb im Sinne des ArbVG muss über ArbeitnehmerInnen verfügen.
4. **Betriebsmittel**; sie sind nicht bloß materieller Natur (EDV-Ausstattung), sondern können auch immaterieller Natur (Know-how) sein.
5. Unter **Betriebszweck** wird der unmittelbare, insbesondere technische Zweck ohne Rücksicht auf den kaufmännischen Erfolg verstanden.
6. **Dauercharakter**; eine Arbeitsstätte kann nur dann ein Betrieb sein, wenn sie auf Dauer angelegt ist. Nicht jede Arbeitsstätte ist daher zugleich ein Betrieb.

Innerhalb eines Betriebs verfolgt also eine physische oder juristische Person oder eine Personengemeinschaft mit technischen oder immateriellen Mitteln die Erzielung bestimmter Arbeitsergebnisse, und zwar fortgesetzt. Es ist gleich, ob Erwerbsabsicht besteht oder nicht.

**Unternehmensbegriff**

Vielfach werden die Begriffe Betrieb und Unternehmen vermischt. Beim Unternehmen steht die wirtschaftliche, beim Betrieb die organisatorische Komponente im Vordergrund. Das Unternehmen wird durch die **zentrale kaufmännische Verwaltung**, das einheitliche Hinarbeiten auf einen bestimmten **wirtschaftlichen Erfolg** charakterisiert. Der Betrieb hingegen ist gekennzeichnet durch die organisatorische Zusammenfassung von Betriebsvorgängen zu einem in sich abgeschlossenen Arbeitsverfahren, die auf Dauer bestimmte Vereinigung von Arbeitskräften zur Erzielung bestimmter Arbeitsergebnisse.

**Filialbegriff**

Ähnliches gilt für die Begriffe Betrieb und Filiale. Filialbetriebe sind nur dann eigenständige Betriebe, wenn sie auch selbstständig bestehen könnten. Es kommt auf die organisatorische Selbstständigkeit an.

## 8.2 Betriebsvereinbarung (BV)

**gesetzliche Verpflichtung zur Zustimmung des Betriebsrates/rätin**

In Betrieben mit Betriebsrat ist die Betriebsvereinbarung (BV) Voraussetzung dafür, dass bestimmte Datenanwendungen vorgenommen werden dürfen. Vor der Einführung folgender Maßnahmen muss die Geschäftsleitung die Zustimmung des Betriebsrates einholen:

- Personalfragebögen, sofern in diesen nicht bloß die allgemeinen Angaben zur Person und Angaben über die fachlichen Voraussetzungen für die beabsichtigte Verwendung des Arbeitnehmers enthalten (§ 96 Abs. 1 Z 2 ArbVG);
- Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren (§ 96 Abs. 1 Z 3 ArbVG);
- leistungsbezogenen Prämien und Entgelten sowie der maßgeblichen Grundsätze (Systeme und Methoden) für die Ermittlung und Berechnung dieser Löhne bzw. Entgelte (§ 96 Abs. 1 Z 4 ArbVG);
- Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen (§ 96a Abs. 1 Z 1 ArbVG);
- Systemen zur Beurteilung von Arbeitnehmern des Betriebes, sofern mit diesen Daten erhoben werden, die nicht durch die betriebliche Verwendung gerechtfertigt sind (§ 96a Abs. 1 Z 2 ArbVG).

Viele Verhaltenskodizes (siehe Kapitel 8.4) enthalten aber Regelungen, die nur mittels BV rechtmäßig vereinbart werden können. Der/die Betriebsrat/rätin muss daher intervenieren, sollten solche Regelungen mittels Verhaltenskodizes eingeführt sein (z.B. Blanko-Unterschriften). Der **Vorteil einer BV gegenüber Verhaltenskodizes** liegt darin, dass sie unter Beiziehung des Betriebsrates entstehen und daher auch die Interessen der Belegschaft beinhalten, rechtsverbindlich und einklagbar sind. Das österreichische Recht gibt dem Betriebsrat gute Voraussetzungen in die Hand, um seine Mitspracherechte wahrzunehmen. Auf diese sollte man nicht verzichten.

## Vorgehensweise

Der Weg zu einer Betriebsvereinbarung in Bezug auf den Transfer von Personaldaten ist meist lange. Zu Beginn ist das elektronische Datenverarbeitungssystem, das neu eingeführt oder erweitert werden soll mitsamt seinen Lücken und Tücken noch unbekannt. Damit hat der Betriebsrat entweder die Möglichkeit Dingen zuzustimmen, über deren Auswirkung er/sie noch wenig Bescheid wissen kann oder er/sie schließt vorerst keine BV dazu ab und hofft, das nach Implementierung des Systems nachholen zu können. Beide Lösungen sind nicht befriedigend. Daher wurde das **„Meilenstein-Konzept"** entwickelt. Die Einführung eines neuen Systems erfolgt dabei in Form eines Projektes. Es werden „Meilensteine" festgelegt, bei denen die Mitbestimmung durch den Betriebsrat erfolgt. Die Entscheidungen werden immer dann getroffen, wenn der jeweilige Projektschritt durchgeführt wird. Meilensteine können z.B. sein:

1. Erarbeitung einer groben Rahmenstruktur, wie das System ausgestaltet sein soll (BR)
2. Auswahl und erste Präsentation eines neuen Systems (GF)
3. Zustimmung/Ablehnung/Veränderung des ersten Vorschlages (BR)
4. Erarbeitung eines Projektplanes zur Implementierung inkl. detaillierter Planung von Datenanwendungen, Zugriffsmöglichkeiten, Testläufen,… (GF)
5. Zustimmung/Ablehnung/Veränderung (BR)
6. Testlauf (GF)
7. Zustimmung/Ablehnung/Veränderung (BR)
8. Gemeinsame Freigabe des Systems und Abschluss der Betriebsvereinbarung (BR und GF)

## Verhandlungsteam

Voraussetzung ist eine Projektgruppe, die diesen Prozess kontinuierlich begleitet. Der Zeitrahmen darf nicht zu eng gesteckt werden. Die an der Projektgruppe beteiligten Personen brauchen einen adäquaten Wissensstand, d.h. dass eventuell **Weiterbildungen** eingeplant gehören und/oder Termine mit **ExpertInnen** vorgesehen werden. Eine begleitende **Mediation** kann der Projektgruppe in Konfliktsituationen weiter helfen.


**Fragen an die Geschäftsführung zum geplanten Datentransfer**

- Welche personenbezogenen Daten sollen übermittelt werden? (taxative Aufzählung der einzelnen Daten, Verwendungszweck pro Datum)
- In welchem System sollen die Daten gespeichert und verarbeitet werden? (Bezeichnung des Systems incl. Version, Vorlage der Systembeschreibung)
- Welche personenbezogenen Auswertungen sollten gemacht werden? (taxative Aufzählung der geplanten Auswertungen, Verwendungszweck pro Auswertung)
- Sollen die Daten mit anderen Daten verknüpft werden? Wenn ja, mit welchen? (Geplante Verknüpfungen, Schnittstellen mit anderen Anwendungen bzw. Systemen? Verwendungszweck)
- Sind Übermittlungen der Daten an Dritte geplant? Wenn ja, welche? (Empfänger innerhalb und außerhalb des Konzerns, Verwendungszweck)
- Wann sollen die Daten gelöscht werden? (Speicherdauer)
- Wer hat Zugriff auf die personenbezogenen Daten? (Aufzählung der Personen bzw. Funktionen mit Zugriff auf welche Daten, Zugriffsberechtigungsplan)
- Wer hat Zugriff auf die Auswertungen? (Aufzählung der Personen bzw. Funktionen mit Zugriff auf welche Auswertungen, Zugriffsberechtigungsplan)
- Wer hat Zugriff auf die erstellten Verknüpfungen? (Aufzählung der Personen bzw. Funktionen mit Zugriff auf die erstellten Verknüpfungen, Zugriffsberechtigungsplan)
- Wer ist für den Datenschutz verantwortlich? (Datenschutzbeauftragter? Datenschutzkonzept?)
- Wie kann der Betriebsrat die Verwendung der personenbezogenen MitarbeiterInnendaten kontrollieren?
- Wie können die MitarbeiterInnen die Verwendung der über ihre Person gespeicherten Daten kontrollieren?
- Wurde eine Meldung an die Datenschutzkommission gemacht? Wurde die Datenanwendung genehmigt?

**Grundsätze für eine gute BV**
**Aktualität**

Die Betriebsvereinbarung sollte immer wieder an die neuen Releases der Datenverarbeitungs-Software angepasst werden (Aktualität). Jede neue Software enthält neue Fehler. Das Programm muss daher **vor dem Einsatz ausreichend geprüft** werden.

**Wissenstransfer**

Allerdings nützt es wenig, wenn Betriebsvereinbarungen die zwischen Betriebsräten und Geschäftsführung abgeschlossen wurden, zwar auf dem neuesten Stand sind, die handelnden Personen, sprich die MitarbeiterInnen aber nicht. Viele Fehler entstehen aus Unkenntnis oder mangelndem Problembewusstsein und nicht aus böser Absicht. Eine **Schulung der MitarbeiterInnen** zu den jeweils aktuellen Datenschutzvorkehrungen und policies ist daher notwendig.

**Löschungsvereinbarungen**

Die Betriebsvereinbarung muss eindeutige Regelungen dazu enthalten, was mit den MitarbeiterInnendaten passiert, sollte jemand **aus dem Betrieb aussteigen**. Wann werden die Daten gelöscht? Wie werden sie entsorgt? Jede Art von Daten, die irgendwann einmal gespeichert wurde, sollte auch irgendwann einmal wieder gelöscht werden. Daten, die falsch sind, und Daten, die nicht mehr benötigt werden, sind zu löschen (§ 27 Abs. 1 und § 28 DSG). Klar ist, dass Stammdaten sowie Daten, die aus gesetzlichen Verpflichtungen heraus gespeichert werden müssen, so lange verwendet werden, solange der/die MitarbeiterIn im Unternehmen ist - vorausgesetzt sie sind richtig. Wie lange aber werden die Unterlagen des Bewerbungsgespräches aufbewahrt? Wie lange werden die Daten aus den MitarbeiterInnen-Gesprächen gespeichert? Bis zum Austritt der MitarbeiterIn aus dem Unternehmen - oder sogar darüber hinaus? Ein Jahr? Fünf Jahre? Dazu muss es verbindliche Vereinbarungen geben.

**Krisenszenarien**

Betriebsvereinbarungen sehen häufig vor, dass im Notfall/Krisenfall besondere Bestimmungen zum Tragen kommen. Diese Sonderbestimmungen unterwandern in der Regel den individuellen Datenschutz stärker, als die Bestimmungen für den Normalfall. Der Betriebsrat muss darauf achten, dass die „Krisensituation" ausreichend definiert ist, sonst liegt die Definition bei der Geschäftsführung und die laxen Regelungen, die für „Krisen" geschaffen wurden, können dann auch für alltägliche Situationen missbraucht werden. **Notfallchecklisten** für jedeN MitarbeiterIn geben klare Verhaltensregeln vor und helfen somit bei der Schadensbegrenzung. Was ist im Falle des Falles konkret zu tun? Wie sollen sich die MitarbeiterInnen verhalten, wenn die Geschäftsführung einen Notfall ausruft? Dürfen dann weiterhin E-Mails verschickt werden? An wen wende ich mich, wenn meine Daten in die falschen Hände geraten sind?

**klare Verantwortlichkeiten**

Klare **AnsprechpartnerInnen** innerhalb des Konzerns helfen, die Datenschutzbelange besser durchsetzen und koordinieren zu können. Die Zuständigkeiten der handelnden Personen müssen dabei klar festgelegt sein. Je nach betroffenen Gruppen (z.B. KundInnen, MitarbeiterInnen) können das auch unterschiedliche Personen sein. Jedenfalls sollte die verantwortliche Stelle einfach zu finden und im Betrieb **bekannt sein**.

**angepasst ans Unternehmen**

Beim Abschluss einer Betriebsvereinbarung muss der/die Betriebsrat/-rätin immer auf die Spezifika des Unternehmens eingehen. Die Vereinbarung sollte nicht zu einer „Abschreibübung" werden, sonst gehen Datentransfers an dem/der ungeschulten Betriebsrat/-rätin vorbei. **Selbstständiges Handeln** ist gefragt und gerade bei diesem komplexen Thema äußerst schwierig. Die GPA-djp Abteilung Arbeit & Technik, sowie die Rechtsabteilung (Kompetenzzentrum Datenschutz) unterstützt die Prozesse zu Betriebsvereinbarungen im Bereich Datenschutz gerne.

**Transparenz**

Damit die Betriebsvereinbarung auch gelesen wird, damit die Belegschaft über ihre Rechte Bescheid weiß, ist es generell notwendig, dass sie nicht zu lang ist und in einer **verständlichen Sprache** abgefasst wird.

**Muster für eine österreichische Konzern-Betriebsvereinbarung**

Geltungsbereich

- alle betroffenen MitarbeiterInnen

Gegenstand der Vereinbarung

- Die Übermittlung von Personaldaten aus den rechtlich eigenständigen Niederlassungen Österreichs an das globale System.
- Die Weitergabe dieser Informationen vom globalen System an IT-Drittsysteme.
- Das Zugänglichmachen der Personalinformationen durch das globale System.

Zielsetzung der Datenverarbeitung

- Möglichst genaue Angabe des/der Verwendungszweck/e.

Datenverwendung

- Umfang der Datensammlung: die zu übermittelten Daten werden in einer Anlage taxativ aufgezählt.
- Frequenz der Datenaktualisierung: durch die lokalen Personaladministrationssysteme, z.B. monatlich.
- Umfang der Datenverarbeitung: die zulässigen Auswertungen werden in einer Anlage taxativ aufgezählt.
- Weitergabe der Daten an Drittsysteme: Aufzählung der Systeme, an die Übermittlungen zulässig sind, Festlegen der Verantwortlichen für die Einhaltung des Datenschutzes in diesen Drittsystemen und Notwendigkeit einer Vereinbarung mit diesen.
- Weitergabe der Daten über die Landesgrenzen hinweg: Zulässig nur in Länder, die einen vergleichbaren Datensicherheitsstandard haben.

Zugriffsregelungen

- Genauer Zugriffsplan (Anlage), der sachlich begründet ist, Zugriff nur auf Datenarbeiten, die für die Tätigkeit der jeweiligen Funktion erforderlich ist, Unterscheidung zwischen personalisierten und anonymisierten Reports.

Training

- Umfasst u.a. Datenschutzbelange, Unterzeichnung einer Erklärung zur Vertraulichkeit durch die Systembenutzer.

Löschregelung

- Die Daten dürfen nur so lange aufbewahrt werden, wie für den Verwendungszweck erforderlich.

Rechte der MitarbeiterInnen

- Einsichtsrecht und Recht auf Richtigstellung der Daten zur eigenen Person.

Rechte des Betriebsrates

- Änderungen der Datenermittlung, -verarbeitung und -übermittlung bedürfen des Einvernehmens mit dem Betriebsrat.
- Recht auf Überprüfung des Systems in Bezug auf Einhaltung der Betriebsvereinbarung, dazu Recht auf Beiziehung eines/r Experten/in, Ansprechperson, die Fragen beantwortet und Zugriff gewährt.
- Recht auf Qualifizierung eines BR-Mitgliedes auf Kosten des Arbeitgebers.
- Schlichtungskommission für Konflikte bezüglich Zulässigkeit von strittigen Datenverwendungen.

Soziales Audit

- Der Betriebsrat erhält regelmäßig Informationen über die Erfahrungen im laufenden Betrieb. Der Umfang dieses Datenschutzberichtes wird mit dem Betriebsrat vereinbart.

## 8.3 Datenschutz-Audit

**Überprüfung der BV durch ein Audit**

Das Abschließen einer BV zum innerbetrieblichen Datenschutz alleine sorgt nicht immer zugleich auch für ausreichenden Datenschutz. Die Einhaltung der BV muss auch kontrolliert werden. Dabei hilft das Datenschutz-Audit. Es kann entweder in Form eines Eigenaudits durchgeführt werden oder als externe Kotrolle durch akkreditierte AuditorInnen durchgeführt werden.

**Protokollierung und Dokumentation**

Schriftliches Festhalten von Aufgabenverteilung, Datenverwendungen, Arbeitsaufträgen im Zusammenhang mit Datenschutz, innerorganisatorischen Datenschutzvorschriften, etc. sind nicht nur hilfreich, wenn es um Datensicherheit - und im schlimmsten Fall rechtliche Beweisführung geht - sondern auch **gesetzlich vorgeschrieben** (§ 14 Abs. 2 Z 7 und 8 DSG). Im Rahmen von einzelnen Bausteinen eines Audits zum Datenschutz müssen daher immer auch solche Dokumentationen und Protokollierungen vorgesehen sein.

**Audit-Bausteine**

- **Information** seitens des Managements zu konkreten Durchführungen und Veränderungen (rechtlich, technisch, organisatorisch) zu den Datenschutz-Maßnahmen gewährleisten die Transparenz; am besten wäre es, in der Betriebsvereinbarung festzuschreiben, dass Veränderungen in einem, nur für das Management und den Betriebsrat einsehbaren - Dokument (z.B. im Intranet) regelmäßig dokumentiert werden.
- Regelmäßige **Evaluierungsroutinen** sichern die Nachhaltigkeit und können für laufende Verbesserungen sorgen.
- **Erfahrungsberichte** zu den Datensicherheitsmaßnahmen seitens der Geschäftsführung unterstützen die Erhebung des Status quo und erleichtern die Soll-Ist-Analyse.
- Sammeln der **Beschwerden und Anregungen** der MitarbeiterInnen seitens des Betriebsrates deckt bestehende Lücken im System auf und hilft neue Lösungsansätze zu finden.
- **Protokollierung** von kritischen Datenverwendungen: zwischen Arbeitgeber und Betriebsrat können kritische Datenverwendungen vereinbart werden, die jedenfalls protokolliert werden.
- **Bereitstellen von Fachpersonal** - den BetriebsrätInnen werden betriebsinterne Ansprechpersonen (Systemadministration, IT, Fachbereich) genannt, die für Auskünfte und zur Vorbereitung eines Audits regelmäßig zur Verfügung stehen.

## 8.4 Verhaltenskodex

**rechtliche Stellung**

Rein rechtlich stellt ein Verhaltenskodex eine **Arbeitsanweisung** dar, die vom Arbeitgeber einseitig erlassen wurde. Die Regelungen werden aber nur insoweit rechtlich verbindlich, als sie dem nationalen Recht und insbesondere dem Arbeitsrecht, nicht entgegenstehen. Verschiedene Begriffe für konzerninterne, einseitig erlassenen Regelungen sind im Umlauf: Privacy Statements, Codes of Conduct, Binding Corporate Rules (BCR), Verhaltenskodizes, etc. Sie regeln - unter anderem - den Transfer von und den Umgang mit personenbezogenen Daten. Diese Instrumente sind eine Möglichkeit, Verhaltensregeln für den gesamten Konzern einzuführen.

**Betriebsinteressen im Mittelpunkt**

Meist gehen diese Regelwerke von der (ausländischen) **Konzernzentrale** aus und sollen in den nationalen Niederlassungen umgesetzt werden oder sie beruhen auf Vorstellungen der Geschäftsführung. Während die Geheimhaltungsinteressen des Unternehmens meist großen Raum einnehmen in diesen Statements und die MitarbeiterInnen auf Geheimhaltung von Betriebsgeheimnissen mehrfach hingewiesen werden, wird mit der Geheimhaltung von MitarbeiterInnen-Daten weniger streng umgegangen.

**Aufgabe des Betriebsrates**

Der Betriebsrat muss acht geben, dass die **Interessen der Belegschaft** darin gewahrt sind. Der Europa- oder Weltbetriebsrat kann sich in die konzernweiten verbindlichen Standards einmischen und seine Forderungen einbringen, wie der Datentransfer gehandhabt werden soll.

**spezielle Inhalte**

Vorschriften zum **Umgang mit elektronischen Kommunikationseinrichtungen** sind häufig in Verhaltenskodizes enthalten. Nicht selten ist dabei auch von Überwachungs- und Kontrollmaßnahmen die Rede, die nach österreichischem Arbeitsrecht zustimmungspflichtig sind. Ein Beispiel dafür ist etwa die Kontrolle von Internet- und E-Mail-Nutzung. In diesen Fällen muss der Betriebsrat einfordern, den Verhaltenskodex an das österreichische Arbeitsrecht anzupassen bzw. allfällig notwendige Betriebsvereinbarungen abzuschließen.

## Exkurs: Whistle-blowing-Hotline

Ein weiteres Beispiel, das häufig in Verhaltenskodizes vorkommt, ist die Einrichtung von so genannten **Whistle Blowing-Systemen** mit **Ethik-Hotlines**, über die MitarbeiterInnen andere „verpfeifen" können. In den USA wurde im Zuge von Bilanzfälschungsskandalen (Enron) ein Gesetz verabschiedet, das von börsennotierten Unternehmen die Einrichtung interner Kontrollmaßnahmen verlangt. US-amerikanische Konzerne sind somit gezwungen, auch bei ihren europäischen Tochtergesellschaften Whistle Blowing-Hotlines einzurichten, damit Unregelmäßigkeiten vor allem in der Buchhaltung und Bilanzierung von KollegInnen (auch anonym) direkt bei der Konzernleitung „angezeigt" werden können.

In Europa wirft dies allerdings sowohl arbeits- als auch datenschutzrechtlich jede Menge Probleme auf. Whistle Blowing und Ethik-Hotlines sind in Österreich nicht ohne weiteres zulässig. Der Arbeitgeber ist jedenfalls verpflichtet, das Whistle-Blowing-System beim Datenverarbeitungsregister zu melden bzw. um Vorabgenehmigung durch die Datenschutzkommission anzusuchen. Weiters ist eine Betriebsvereinbarung nach § 96 Abs. 1 Z 3 ArbVG erforderlich, da ein Whistle Blowing-System eine Kontrollmaßnahme darstellt, die geeignet ist, die Menschenwürde zu berühren. In einer solchen Betriebsvereinbarung sollte ein ausgewogenes Verfahren verankert werden, mit welchem „Anzeigen" behandelt werden und der Betriebsrat eine Kontrollfunktion hat, um die Persönlichkeitsrechte der MitarbeiterInnen zu wahren.

Um sicher zu gehen, dass Verhaltensvereinbarungen das Papier wert sind, auf dem sie geschrieben sind, hilft die Checkliste auf der Folgeseite ➜

**Merkmale einer guten Regelung zum Datenschutz**

1. **Beschränkung der Zweckbestimmung** - Die Daten dürfen nur für einen bestimmten Zweck verwendet werden. Dieser ist festgelegt und darüber hinaus ist jede Datenanwendung untersagt.
2. **Qualität und Verhältnismäßigkeit** - Die Daten müssen aktuell sein und sie müssen den Zweck, für den sie bestimmt sind, auch erfüllen können. Eine umfangreiche Übermittlung von Daten, die nichts mit dem angegebenen Zweck zu tun hat, ist verboten.
3. **Weitergabe an Dritte beschränken** - Die Daten dürfen nicht an Dritte weitergegeben werden, außer diese sind mittels Vertrag eindeutig verpflichtet dasselbe Datenschutzniveau zu bieten, wie im Ausgangsland.
4. **Speicherzeit** - Es muss festgelegt werden, wie lange welche Daten gespeichert werden sollen. Das gilt insbesondere für Verträge mit Dritten oder Dienstleistern zur Datenverarbeitung.
5. **Transparenz** - Die betroffenen Personen haben das Recht, informiert zu werden. Sie kennen ihre AnsprechpartnerInnen und sie wissen, welche Sanktionen das handeln gegen die Vereinbarung mit sich bringt.
6. **Verständlichkeit** - Die Vereinbarung muss so verfasst sein, dass sie allgemein verständlich ist, was z.B. durch Praxisbeispiele erleichtert wird.
7. **Zugriff, Berichtigung, Widerspruch** - Die Betroffenen haben das Recht, ihre Daten zu sehen und im Falle des Falles richtig zu stellen.
8. **Sicherheit** - Technische und organisatorische Maßnahmen müssen getroffen werden. Die Datenverarbeitenden dürfen nur auf Anweisung der Verantwortlichen arbeiten.
9. **Unterstützung** - Die Vereinbarung enthält Unterstützung und Hilfestellung für die Betroffenen, was u.a. mittels eines klaren Instanzenweges bei Missständen und Beschwerden gewährleistet werden kann. Die Institutionen (z.B. eine interne Schlichtungsstelle) müssen neutral sein (d.h. nicht abhängig von den handelnden Personen bzw. paritätisch besetzt), Kontrollbefugnisse haben und leicht zugänglich sein (d.h. möglichst nicht auf Kosten derjenigen arbeiten, die eine Beschwerde einreichen).
10. **Entschädigung** - Bei nachgewiesenen Missbrauch werden die Betroffenen entschädigt, was auch in finanzieller Hinsicht geregelt sein kann. Eine Schädigung ist nicht allein bei materiellem Schaden oder Verlust gegeben sondern betrifft auch psychische und moralische Schäden.
11. **Befolgungsrate** - Diese muss hoch sein. Die Vereinbarung wird auch von den handelnden Personen eingehalten, was durch regelmäßige externe Überprüfung (z.B. Audits, Zertifizierungs-Gremien, etc.) erfolgen kann und auch mittels klarer Sanktionsmechanismen gefördert wird (z.B. über die gesetzlichen Verbindlichkeiten hinausgehender Schadensersatz für Betroffene bei Nicht-Einhaltung der Vereinbarung). Eine rein auf freiwilliger Basis eingeführte Vereinbarung hat aller Voraussicht nach wenig Aussicht auf Erfolg. Die Konsequenzen für Fehlverhalten müssen bekannt gemacht werden. Wird ein Datenmissbrauch bekannt, sollte er auch tatsächlich sanktioniert werden.
12. **Bewusstsein und Überprüfung** - Voraussetzung für eine hohe Befolgungsrate ist, dass die Betroffenen von der Vereinbarung wissen und sie auch inhaltlich kennen. Das kann z.B. über regelmäßige Schulungen, Wissensabfragen u.ä. gefördert werden.
13. **Nachhaltigkeit und Überprüfung** - Die Wirksamkeit der Maßnahmen zur Datensicherheit muss regelmäßig einer Überprüfung unterzogen werden (z.B. Audit). Die Verhaltensvereinbarung kann als kontinuierlicher Prozess gesehen werden, der immer wieder der Aktualisierung bedarf.
14. **Sensiblen Daten** - Bei sensiblen Daten müssen die Betroffenen persönlich der Verwendung zustimmen.
15. **Direktmarketing** - Beim Direktmarketing muss der/die Betroffene jederzeit die Zustimmung widerrufen können.

**Angebot der OECD**

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat ein Instrument entwickelt, das automatisch derartige Selbstverpflichtungserklärungen kreiert, den **„OECD-Privacy Policy Generator"** (Link dazu findet sich im Anhang). Damit können Anbieter im Internet - angepasst an ihre Webpages - eigene Statements kreieren. ACHTUNG: dieses automatische Instrument garantiert nicht, dass damit auch den nationalen Datenschutzregelungen entsprochen wird! Es gewährleistet auch nicht, dass diese „Statements aus der Retorte" dann auch wirklich eingehalten werden.

## 8.5 DatenschutzbeauftragteR (DSB)

**internationale Rechtslage**

Im Unterschied beispielsweise zum deutschen[6], französischen, tschechischen, ungarischen oder slowakischen Datenschutzgesetz kennt das österreichische Recht keine Verpflichtung zur Ernennung oder Einstellung von Datenschutzbeauftragten (DSB). In einigen EU-Ländern sind die **Voraussetzungen** für die Bestellung zum/zur Datenschutzbeauftragten umfangreich gestaltet (z.B. Tschechische Republik, Slowakei). Die KandidatInnen müssen ein Universitätsstudium absolviert haben, langjährige Berufserfahrung im Fachgebiet vorweisen und unabhängig von politischen Parteien sein. Sowohl in punkto Ausbildung als auch in punkto Unabhängigkeit haben die meisten westlichen EU-Staaten hier Nachholbedarf.

**Ausbildung der DSB**

Nachdem das österreichische Gesetz keine DSB vorsieht, kennt es auch keine Ausbildungsgrundsätze für DSB. Folglich ist die innerbetriebliche Ausbildungspraxis höchst unterschiedlich. In einigen wenigen Betrieben sind Datenschutzbeauftragte etabliert. Die DSB haben Seminare von einem halben Tag bis zu einer Woche absolviert, um auf ihre Tätigkeit vorbereitet zu werden. Das ist eine höchst heterogene und unzureichende Grundlage für so eine komplexe Materie.

**Aufgaben der DSB**

Außerdem ist das Aufgabengebiet der DSB meist stärker auf KundInnendaten fokussiert als auf MitarbeiterInnendaten. Es ergibt sich von selbst, dass diese Vorgehensweise problematisch ist und die Interessen der ArbeitnehmerInnen nicht wirklich geschützt sind. (Welche Rechte und welches Tätigkeitsprofil die GPA-djp für Datenschutzbeauftragte fordert, ist in Kapitel 10 dargestellt.)

## 8.6 Sicherheitsmanagement

**rechtliche Grundlage**

Datenschutzrechtliche Sicherheitsbestimmungen sind im § 14 des DSG festgelegt. Der Gesetzgeber verlangt, dass die Sicherheitsmaßnahmen im wesentlichen drei Kriterien entsprechen. Sie müssen:

1. Angepasst an den Stand der Technik,
2. wirtschaftlich vertretbar sein und
3. ein angemessenes Schutzniveau erreichen.

Der „Stand der Technik" ist gerade in der sich rasch wandelnden IKT-Branche schwierig auszulegen. Der Ausdruck „wirtschaftlich vertretbar" wird seitens der Geschäftsführung gerne gleich gesetzt mit „darf nichts kosten". Das kann allerdings nicht argumentiert werden - es muss sehr wohl ein Budget für Sicherheitsmaßnahmen zur Verfügung gestellt werden. Was fehlt, sind Verhaltensvorgaben sowie technische und organisatorische Standards zum Datenschutz. Die Gesetzesbestimmungen zur Datensicherheit also nicht ausreichend.[7]

---

[6] In Deutschland ist der Datenschutzbeauftragte stark föderalistisch organisiert. Das bedeutet, dass jedes Land eine eigene Gesetzgebung und eine eigene Behörde zum Datenschutz hat. Die einzelnen Länder praktizieren daher unterschiedlich fortschrittliche Methoden im Datenschutz. Schleswig-Holstein beispielsweise gilt als sehr modern.

[7] Im Gegensatz zu Österreich hat Deutschland beispielsweise ein konkretes Gütezeichen zur IT-Sicherheit.

**empfohlene Sicherheitsmaßnahmen**

Was das Gesetz zwar nicht vorschreibt, aber als technische Standards empfohlen wird (unter anderem von der ARGE Daten) um sich keine Haftungsprobleme einzuhandeln sind:

- Zertifizierung der Website;
- Verschlüsselung von Mitteilungen;
- Virenfilter, Spamfilter, Webfilter;
- Firewall;
- Backup-Kopien;
- SSL-Online Formulare, Mail- Encryption;
- W-LAN-Sicherheitsmaßnahmen (z.B. Verschlüsselung, Passwort);
- Virtual Private Network Lösung (VPN).

Um für alle Bereiche, Abteilungen und Einheiten eines Unternehmens datenschutzrechtlich einwandfrei gerüstet zu sein, empfiehlt es sich, ein Sicherheits-Management für den gesamten Betrieb zu entwickeln. Die Schritte zu einem erfolgreichen Information-Security-Management-Systems (ISMS) sind:

**Vorgehensweise**

1. IT-Strukturanalyse des Ist-Zustandes; Welche Systeme und Anwendungen werden verwendet? Inventarliste aller Hard- und Software im Unternehmen erstellen.
2. Feststellen des Schutzniveaus; Welche Daten werden verwendet und welche gesetzlichen Schutzmaßnahmen sind für diese Daten vorgesehen? Soll das Unternehmen über den gesetzlichen Standard hinausgehende Schutzmaßnahmen ergreifen?
3. Analyse des Sicherheits-Bedarfs (Soll-Ist-Vergleich); dabei helfen das Österreichische Informationssicherheitshandbuch oder der IT-Grundschutz-Katalog (siehe folgende Seite)
4. Auswahl der Sicherheitsmaßnahmen
5. Konsolidierung der Maßnahmen
6. Realisierung der Maßnahmen
7. Regelmäßige Kontrolle der Maßnahmen

Was hier in aller Kürze dargestellt ist, bedarf in der Regel mehrerer Monate - wenn nicht sogar Jahre - intensiver Arbeit und Auseinandersetzung. Um festzustellen, ob im Betrieb auf Datensicherheit geachtet wird, hilft die folgende Checkliste:

**Sicherheitscheckliste**

Gibt es ein Sicherheitskonzept? Hat die Geschäftsführung klare Ziele und Richtlinien zum Schutz personenbezogener Daten festgelegt?
Ist das Konzept betriebsintern bekannt? Sind die Ziele und Richtlinien den MitarbeiterInnen, SystemadministratorInnen, Empfängern, und anderen relevanten Personengruppen bekannt?
Werden die MitarbeiterInnen beim Eintritt ins Unternehmen hinsichtlich Datenschutz geschult? Unterschreiben alleine genügt nicht!
Werden die MitarbeiterInnen regelmäßig auf den neuesten Stand gebracht? Gibt es Maßnahmen zur Erhöhung der Sensibilität in punkto Datenschutz?
Ist klar, wie mit den personenbezogenen Daten beim Austritt eines/r MitarbeiterIn umzugehen ist?
Gibt es eine Dokumentationspflicht zu Maßnahmen der Datensicherheit? Diese erleichtern die Kontrolle und Beweissicherung im Streitfall.
Sind die Verantwortungsbereiche festgelegt? Gibt es Datenschutzbeauftragte? Gibt es Vertretungen für die jeweiligen Verantwortungsbereiche?
Sind die wichtigsten Datenanwendungen inventarisiert? Ist den AnwenderInnen der Schutzbedarf klar?
Werden die Schutzmaßnahmen regelmäßig aktualisiert? Medikamente haben ein Verfallsdatum - Viren-Schutzprogramme auch!
Werden die Schutzmaßnahmen kontrolliert?
Wird ein Fehlverhalten sanktioniert?
Sind die allfälligen Sanktionen den MitarbeiterInnen bewusst?

**Verantwortung der Geschäftsführung**

Auf jeden Fall ist der Auftraggeber auch für die Sicherheitsmaßnahmen verantwortlich.

**Beispiel aus der Rechtsprechung**
Der OGH entschied 1990, dass die Erstellung eines Sicherheitskonzeptes zu den Kernaufgaben des Managements zählt. Ein ehemaliger Mitarbeiter war an der Entwicklung einer Software beteiligt. Die Dokumentation der Entwicklung wurde erst nach seinem Weggang begonnen. Die Programmteile, die der Mitarbeiter entwickelt hatte, waren aber nicht mehr auffindbar. Die Firma wollte die Rekonstruktionskosten mit den Abfertigungsansprüchen des ehemaligen Mitarbeiters gegenrechnen. Der OGH hat das untersagt - ein nicht vorhandenes Sicherheitskonzept kann nicht zu Lasten der MitarbeiterInnen ausgelegt werden (OGH Entscheidung 9 Ob 182/90).

**Literaturhinweise**

Für einen grundlegenden Überblick zum betriebsinternen Sicherheitsmanagement eignet sich das Handbuch des Bundeskanzleramtes, **„Das Österreichische Informationssicherheitshandbuch"**. Darin werden Methoden und Vorgehensweisen zur Datensicherheit dargestellt (http://www.digitales.oesterreich.gv.at). Seit Juni 2007 ist die Anwendung des Handbuch im öffentlichen Dienst per Ministerratsbeschluss empfohlen.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt sich seit 1991 mit Forschung und Informationspolitik zum Thema Datensicherheit. Im Laufe der Jahre wurde ein Instrument entwickelt, das im Baukastensystem konkrete Maßnahmen zum Datenschutz anbietet - der **„IT-Grundschutz-Katalog"** (http://www.bsi.bund.de/gshb/deutsch/index.htm). Die Verwendung der Bausteine und Maßnahmen ist für Ungeübte eher schwierig, da das Material sehr umfangreich ist. Für den Transfer von MitarbeiterInnen-Daten sind beispielsweise folgende Bausteine unter dem oben angegebenen Link relevant:

➜ Bausteine ➜ Anwendungen ➜ SAP
➜ Maßnahmenkataloge ➜ Personal

**Zertifizierung als Sicherheitsmaßnahme**

Nur neun Unternehmen in Österreich haben sich bisher bis zu einer Zertifizierung ihrer IT-Sicherheit nach **ISO-Norm 27001** vorgewagt (z.B. Bundesrechenzentrum, Kapsch, Raiffeisen Informatik, Siemens IT Solutions, Telekom Austria). Zertifiziert werden kann auch nach dem in Deutschland entwickelten **BSI-Standard 100-1, 100-2 und 100-3**. Hier sind vorwiegend Behörden erfasst aber auch einige Unternehmen (z.B. BFI Wien, ÖBB, Statistik Austria, TU Graz, Verbund).

Die Kosten für eine derartige Zertifizierung sind schwierig abzuschätzen - je nachdem ob man die durchzuführenden Schritte mit berechnet oder rein das Verfahren. Man muss aber mindestens mit 4.000 EUR für PrüferInnen und Abwicklung rechnen.

**beratende und zertifizierende Unternehmen**

Beratend zur IT-Sicherheit sind in Österreich derzeit etwa sechs Unternehmen aktiv. Zertifizierungen im Datenschutz werden derzeit in Österreich von zwei Unternehmen angeboten; „A-cert" und „CIS - Certification & Information Security Services GmbH".

**Grundsätze der Zertifizierung**

Egal nach welcher Norm und egal bei welchem Zertifizierungsunternehmen, die zentralen Bestandteile eines Information-Security-Management-Systems sind:

- Protokollierung
- Kontrolle
- Kontinuierliche Verbesserung

## Exkurs: Achtung „kleine" Umfrage!

**Daten sind rückverfolgbar**

„Kleine" Umfragen zur Zufriedenheit mit der Arbeit, dem allgemeinen Gesundheitszustand, der persönlichen Meinung, etc. kommen immer wieder über das Intranet zu den Angestellten. Auch diese Daten können konzernweit gesammelt und ausgewertet werden.

In Abteilungen mit wenigen MitarbeiterInnen ist es nicht weiter schwierig, die „anonymen" Angaben zu einzelnen Personen zurückzuverfolgen. Geschlecht, Dauer der Betriebszugehörigkeit und hierarchische Zuordnung werden angegeben - und schon kann ausgewertet werden, wie ihr höchst persönlicher Gesundheitszustand aussieht.

Die Folgen werden nicht sofort direkt ersichtlich sein, aber vielleicht kommt jemand auf die Idee, ihre Fehlzeiten genauer unter die Lupe zu nehmen und sie als „Risiko" zu beurteilen.

**Beispiel aus der Praxis**

Ein global agierendes Versicherungsunternehmen hat seine Unternehmensstruktur in eine so genannte „Matrixstruktur" geändert. Das heißt, dass die Leitungsfunktionen global vernetzt sind und immer weniger Entscheidungen auf nationaler Ebene gefällt werden können.

Um festzustellen, wie es den in dieser neuen Matrix arbeitenden MitarbeiterInnen persönlich geht, wurde eine anonymisierte Onlinebefragung eingeleitet, auch "Quick Pool" genannt. Der globale Personalchef hatte diese Idee, weil er sehen wollte, wie sich vor allem die EuropäerInnen in dieser Organisationsform fühlen. Es wurde allerdings weder auf europäische Vorschriften noch auf lokale Gesetze (DSG, ArbVG) Rücksicht genommen. Die Betriebsräte wurden nicht informiert. Nicht einmal der österreichische Personalchef wusste davon!

Die MitarbeiterInnen kamen am Montag in der Früh in die Arbeit, klickten ein harmloses Mail an und haben die Befragung - bis auf einige wenige - ausgefüllt. Da das österreichische Legal Departement nur aus einer Person bestand und dies auch ein Jurist war, kamen ihm Bedenken, ob dies rechtens sei. Hintergrund war, vor allem, dass die meisten der abgefragten Abteilungen in Österreich so klein waren, lediglich aus 1-2 MitarbeiterInnen bestanden, sodass sofort eine persönliche Auswertung gemacht hätte werden können. Damit wäre es zu mehrfachen Verstößen gegen das ArbVG, das DSG und gegen interne Betriebsvereinbarungen gekommen. Er wandte sich an den Betriebsrat und dieser sandte umgehend ein Mail an den globalen Head of HR, erinnerte an die Compliance-Verpflichtungen des Unternehmens und drohte mit einem Antrag auf "Einstweilige Verfügung" bei Gericht zur Einstellung dieser anonymen Befragung. Die österreichischen. BetriebsrätInnen konnten durch schnelles Reagieren, die Deutschen und Schweizer KollegInnen, dazu bewegen, die Quick-Pool-Befragungen zumindest in diesen Ländern einzustellen.

Anmerkung: Die nicht so "zimperlichen" KollegInnen in England und Irland haben die Befragung brav ausgefüllt. Das Ergebnis war, dass die MitarbeiterInnen sich durch die Arbeit in der MATRIX persönlich frustriert gefühlt haben und Entscheidungen und ihre Strukturen nicht verstanden wurden. Es hat sich später heraus gestellt, dass angestrebt war, global monatliche Befragungen durchzuführen. Mittlerweile werden diese auch in den nicht "zimperlichen" Ländern immer seltener, weil die befragten MitarbeiterInnen keinen Sinn darin sehen, ständig wiederkehrend, ähnliche Fragen an einen unbekannten, irgendwo in den USA sitzenden Personalchef zu beantworten und Zeit haben sie dafür wohl auch keine mehr.

## Handlungsmöglichkeiten

Sensibilisierte MitarbeiterInnen können den Betriebsrat/-rätin darauf aufmerksam machen, wenn unqualifizierte Umfragen/Tests u.a. Datenerfassungen im Betrieb gemacht werden.

Der/die Einzelne sollte sich dabei folgende Fragen stellen:

- ➜ Weiß der Betriebsrat von der Umfrage? Wenn nicht, dann sollte das rasch passieren.
- ➜ Sind die Daten tatsächlich anonym? Wenn nicht, ist das schleunigst von dem/der Betriebsrat/rätin zu veranlassen.
- ➜ Fragen Sie in der Geschäftsführung/der Personalabteilung, wozu die Umfrage dienen soll.
- ➜ Geben Sie keine Antworten, die Rückschlüsse auf ihre Person zulassen.
- ➜ Tritt so etwas häufiger auf, regen Sie beim Betriebsrat eine Betriebsversammlung an, um die Belegschaft für diese „Datenschnüffelei" zu sensibilisieren.

### Exkurs: Achtung biometrische Datenerfassung!

**Sonderfall biometrische Daten**

Bei der biometrischen Datenerfassung ist die Menschenwürde eindeutig berührt, stellt der Oberste Gerichtshof fest. Eine Betriebsvereinbarung nach § 96 ArbVG ist somit Pflicht! Dort wo die Menschenwürde nicht nur berührt, sondern verletzt ist, ist die Systematik darüber hinaus individuell zustimmungspflichtig. **Die Einzelperson kann dann verhindern, dass ihre Daten biometrisch erfasst werden, indem sie einem solchen System nicht zustimmt!**

**Beispiel aus der juristischen Praxis (Gesundheitsbranche)**
Die Arbeitszeiterfassung wurde auf eine Methode mittels Fingerscan umgestellt. Der Betriebsrat klagte. Das Erstgericht erließ die beantragte einstweilige Verfügung, das Rekursgericht bestätigte. Der OGH entschied, dass im Gegensatz zu üblichen Zeiterfassungssysteme wie Stechuhren oder Magnetkarten, die die Menschenwürde nicht berühren, die biometrische Erfassung aufgrund der Intensität des Eingriffes und der Kontrolle als Eingriff in die Menschenwürde zu werten ist. Die Arbeitszeiterfassung mittels personenbezogener biometrischer Daten (Fingerscans) darf daher in Unternehmen nicht ohne eine Betriebsvereinbarung eingeführt werden. (OGH, Urteil vom 20.12.2006, 9 ObA 109/06d beruft sich auf ArbVG § 96, ABGB § 16 und DSG 2000 § 4).

## 8.7 Verschlüsselung von Daten

**Datensicherheit durch Verschlüsselung**

E-Mails passieren auf ihrem Weg zum/zur EmpfängerIn mehrere Stationen (z.B. Server, Router). Damit sie unterwegs nicht in unbefugte Hände geraten, und von unbefugten Augen gelesen werden, kann man die Mails verschlüsseln. Es gibt zwei Systeme, die sehr gebräuchlich bei der Verschlüsselung von Daten sind: „Pretty Good Privacy" (**PGP**) und „GnuPrivacyGuardist" (**GnuPG**). Beide Verschlüsselungssysteme sind kostenlos im Internet erhältlich. Damit werden E-Mails so verschlüsselt, dass nur die EmpfängerInnen sie lesen können - vorausgesetzt er/sie verwendet dasselbe Verschlüsselungssystem.

**technische Vorgehensweise**

Technisch funktioniert die Verschlüsselung bei PGP so, dass ein „Schlüsselpaar" erzeugt wird. Mit dem einen Schlüssel wird kodiert, also die Nachricht quasi versperrt, mit dem anderen Schlüssel wird die Nachricht dekodiert, also entsperrt. Freunde und Bekannte können sich nun gegenseitig als vertrauenswürdig zertifizieren und so ihre Schlüssel austauschen.

Bei **GnuPG** wird nur ein Schlüssel erzeugt, der zwischen den E-Mail-PartnerInnen auf einem sicheren Kommunikationskanal ausgetauscht wird. Man kommt ohne zentrales Netzwerk aus.

Die Systeme sind mitunter in der Installation ein wenig aufwendig, sind aber in technischer Hinsicht äußerst sicher und erfreuen sich daher relativ großer Beliebtheit.

**Literaturhinweis**

Nähere Informationen zu Verschlüsselung und anderen technischen Tools zum Datenschutz finden sich in der Broschüre „Rächer der enterbten Daten" der Interessengemeinschaft work@IT der GPA-djp.

# 9) Argumentarium

**Vorteile der automatisierten Datenverwendung**

Nicht jede Art der Datenverarbeitung ist zu kritisieren. Die Verwaltung von Personaldaten mit elektronsicherer Kommunikationstechnologie hat auch Vorteile (größere Mengen können erfasst werden, Verarbeitung braucht weniger Platz,…). Innerbetriebliche Statistiken helfen, die Situation im Betrieb besser zu erforschen. Die anonyme Weitergabe von Daten einer Einzelperson wäre unbedenklich. Solange die Daten nicht personenbezogen sind und nicht verknüpft werden, sondern zum Beispiel nur zur statistischen Erfassung der Arbeitszufriedenheit dienen, spricht nichts dagegen.

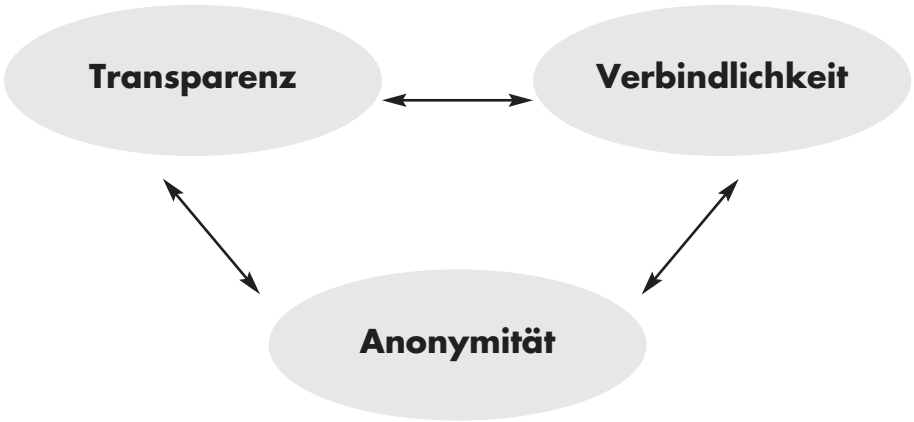
**Probleme Datenanwendungen**

In vielen Fällen wird aber die Datenerfassung und Weitergabe ohne spezifischen Grund und ohne die nötigen Sicherheitsvorkehrungen gemacht. Dass es technisch möglich ist, ist aber kein ausreichender Zweck für umfassende Datensammlungen und -verarbeitungen. Argumente gegen eine solche Vorgehensweise sind im folgenden Kapitel gesammelt.

## 9.1 Für die Belegschaft

**Spannungsfeld**

Der Umgang mit Daten von MitarbeiterInnen bewegt sich immer in einem Spannungsfeld. Es besteht ein Interessenskonflikt zwischen dem Wunsch nach Anonymität und Privatsphäre - auch im Arbeitsleben - und dem Wunsch nach Transparenz und klaren Strukturen. Zugleich sind Verbindlichkeit und Verlässlichkeit ein wesentliches Anliegen der MitarbeiterInnen. Je höher die Transparenz für alle MitarbeiterInnen auf allen Ebenen ist, desto geringer ist wiederum die Möglichkeit, im Gesamtkonzern anonym zu bleiben. Je mehr Verlässlichkeit und Verbindlichkeit besteht, desto höher sind die Anforderungen an die interne Transparenz. In diesem Spannungsfeld gilt es die geeignete Lösung für jedes Unternehmen zu finden. Man muss aber die Vor- und Nachteile genau durchdenken, um die optimale Lösung zu finden. Dabei hilft es, sich dieses Spannungsfeld bewusst zu machen.




**unterschiedliche Bewertung von Daten**

Es wird allerdings ein eklatanter **Widerspruch** deutlich, wenn man sich ansieht, wie mit **betriebsbezogenen Daten** umgegangen wird und wie mit **MitarbeiterInnendaten**. Handelt es sich um Bilanzkennzahlen, KundInnendaten oder andere „Betriebsgeheimnisse“, werden die MitarbeiterInnen hinlänglich auf ihre Geheimhaltungsverpflichtung hingewiesen. Sie müssen Verhaltensvereinbarungen unterschreiben und sich den firmeninternen „commitments“ beugen. In Zusammenhang mit den Daten der MitarbeiterInnen nehmen es die Firmen weitaus weniger genau. Die Geburt eines Kindes wird ungefragt in der Mitarbeiterzeitung veröffentlicht, die Leistungsdaten werden an die ausgelagerte Personalverrechnung weitergegeben, wo völlig unklar ist, wer aller Einsicht nehmen kann und auch Daten wie Alter, Eintrittsdatum in die Firma und Einkommen werden ohne Zustimmung der MitarbeiterInnen übermittelt, um die passende Pensionsvorsorge zu errechnen und das wird dann nicht als „Werbemaßnahme“ sondern als „Service an die MitarbeiterInnen“ verkauft.

**Sensibilisierung im Betrieb**

Je höher das Bewusstsein und das Wissen um Datenschutz innerhalb des Betriebes desto eher wird verhindert, dass MitarbeiterInnen ausgenutzt werden (z.B. Einschüchterungsversuche, Überredungsgeschick). Besteht ein Bewusstsein für Datensicherheit, bleiben sensible und personenbezogene Daten dort wo sie hingehören - im Verantwortungsbereich einiger weniger, mit besonderen Kompetenzen ausgestatteter MitarbeiterInnen.

**gläserne MitarbeiterInnen**

„Ich habe nichts zu verbergen. Meine Daten können sie ruhig haben."

Problematisch wird es bei der Datenverarbeitung wenn eine große Anzahl an Informationen automationsunterstützt verarbeitet und verknüpft wird. Erst im Vergleich mit unzähligen anderen Personaldaten wird einE MitarbeiterIn „auffällig". Die **Beurteilung** von Beschäftigten (z.B. Leistung, Pünktlichkeit) wird mittels solcher Verknüpfungen für den ganzen Konzern vorgenommen und der/die Einzelne weiß aber nicht, was an den anderen Standorten als „pünktlich" gilt oder welche Leistung als angemessen gesehen wird. Bei internationalen Konzernen kommen noch kulturelle Unterschiede bei der Beurteilung hinzu. Mitunter werden dabei „Äpfel mit Birnen" verglichen.

**Beispiel aus der betrieblichen Praxis**
In einem weltweit agierenden Unternehmen werden die Lohndaten aus Österreich und der Slowakei miteinander verglichen. Dabei wird allerdings nicht auf die nationalen Steuergesetze oder die Gesetzesgrundlagen für die Gewährung von Prämien Rücksicht genommen. Es stellt sich die Frage, wie wertvoll ein solcher Vergleich als Grundlage von Performance-Benchmarking ist.

**präventive Maßnahmen gegen Datenmissbrauch**

„Es ist doch noch nie etwas passiert!"
„Und wie oft hatten Sie schon sechs Richtige im Lotto und spielen trotzdem immer wieder?"

Die Gefahr, dass Daten missbräuchlich verwendet werden, ist zwar größer als die Wahrscheinlichkeit, im Lotto zu gewinnen, dennoch macht dieser plakative Vergleich deutlich, worum es geht - Vorsorge ist besser als das Nachsehen zu haben.

Wenn keine Fälle von Datenmissbrauch bekannt sind, kann das genauso gut auch heißen, dass sie bislang niemandem aufgefallen sind oder wenn dann gut vertuscht wurden.

**Objektivität ist relativ**

Um Verzerrungen aufgrund von unterschiedlichen kulturellen Traditionen zu vermeiden, werden manchmal höchstkomplexe Beurteilungssysteme erstellt, die **„objektives"** Vergleichen ermöglichen sollen. Solche „objektiven" Punktesysteme sind aber weit weg von der Realität des/der Einzelnen. Menschen handeln nun einmal nicht ausschließlich nach statistisch messbaren Größen - und das ist für Unternehmen auch manchmal ein Vorteil, wenn z.B. schnell und aufgrund von Erfahrungswissen Entscheidungen getroffen werden müssen. Die eine, reine und einzig wahre Objektivität gibt es nicht. Was in einer Situation von Vorteil ist, kann in der anderen schlechte Auswirkungen haben. Manchen Vorgesetzten gegenüber kann man Kritik äußern und das wird als „Engagement" gewertet, bei anderen wird Kritik als „Illoyalität" gewertet. **Eine zentrale Beurteilungs-Datenbank kann nicht objektiv sein!**

**langläufiges Ziel konzernweiter Datenvergleiche**

Das Ziel von zentralen Personaldatenbanken ist immer der konzerninterne Vergleich, um die Konzernergebnisse zu „optimieren", sprich Kosten zu senken, sprich Angestellte zu entlassen. Das konzernweite Ranking ermöglicht Entlassungen und die Aufgabe von Standorten noch einfacher, da an einer anonymen, „objektiven" Stelle, Personal- und Organisationsentscheidungen getroffen werden, von Menschen die mit den zu Entlassenden keinerlei direkten Kontakt haben.

**Ende der Diskretion**

Daten aus Mitarbeitergesprächen, Weiterbildungswünschen, etc. können zu begehrten Objekten für das zentrale Human-Ressource-Management werden. Die **Diskretion** von Vier-Augen-Gesprächen zwischen MitarbeiterIn und direktem/r Vorgesetzten/r geht so verloren.

**innerbetriebliche Möglichkeiten durch Datenschutz**

Im Zusammenhang mit Regelungen zum internationalen Datenverkehr, kann sich die Gelegenheit zur Aufarbeitung und **Sanierung offener Problemstellungen** und/oder ungeregelter Vorgehensweisen im Betrieb ergeben.

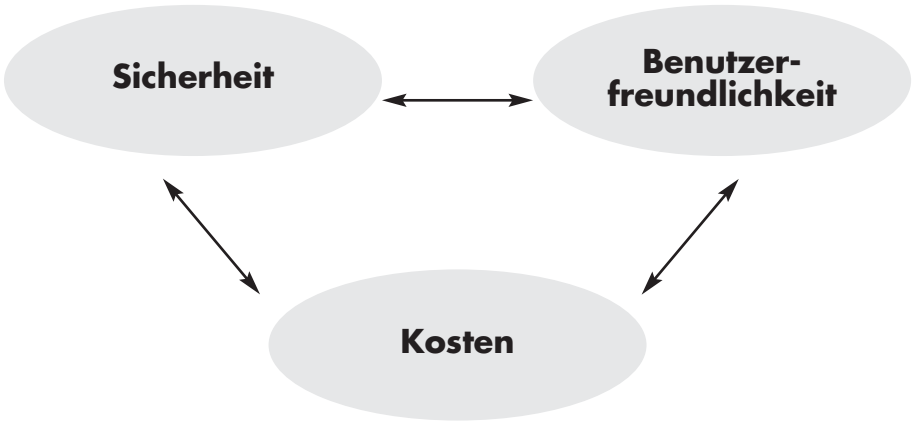
**Verantwortliche**

Rein rechtlich gesehen ist die Datenschutzkommission (siehe Kapitel 5) für die Überprüfung und Kontrolle des innerbetrieblichen Datenschutzes zuständig. Diese Kommission ist jedoch chronisch unterbesetzt, sieht sich mit einem hohen Verwaltungsaufwand konfrontiert und wird somit auf eigene Initiative hin nicht aktiv. Umso mehr ist es erforderlich, dass sich jemand im Betrieb für den Schutz der MitarbeiterInnen-Daten verantwortlich fühlt. Dem **Betriebsrat** kommt hier große Bedeutung zu. Er kann Kraft Arbeitsverfassungsgesetz auch für Datenschutz sorgen. Ein Weg dorthin führt über die Einrichtung eines/r innerbetrieblichen Datenschutzbeauftragten (siehe Kapitel 8.5 und 10).

## 9.2 Gegenüber der Geschäftsführung

**Spannungsfeld**

Nicht nur die Belegschaft befindet sich beim Thema Datenschutz in einem Interessenkonflikt, auch das Management befindet sich in einem Spannungsfeld. Um für Verhandlungen gerüstet zu sein, hilft es, sich das Dilemma der Geschäftsführung vor Augen zu halten. Die Koordinaten, zwischen denen sich die Geschäftsführung bewegt, sind die Datensicherheit, die Bequemlichkeit für die NutzerInnen und AnwenderInnen sowie die Kostenfrage.




**Lassen sie jemanden mit dem Feuerzeug in den Benzintank schauen? - Nein! Warum lassen sie dann Unbefugte in ihre MitarbeiterInnen-Daten schauen?** Beides kann Effekte in ungeahntem Ausmaß haben.

**weniger Kompetenzen**

Ein Datentransfer an eine zentrale Konzerneinheit bedeutet in der Regel, dass die Zuständigkeit der nationalen Einheit damit aufgehoben wird. Die Personalverrechnung wird dann z.B. viele ihrer Aufgaben abgeben müssen - wenn sie nicht gänzlich aufgelöst, sprich entlassen wird. Das bedeutet einen **Machtverlust** für den nationalen Standort. Jedes Outsourcing von Zuständigkeiten heißt, dass die Entscheidungsbefugnisse nun nicht mehr in der Hand derjenigen liegen, die diese Aufgaben Jahre lang erfüllt haben, die sich Kompetenzen angeeignet haben, die nahe am Geschehen sind.

Eine Datenverlagerung bedeutet immer auch, dass die Kompetenzen für die Datenverwaltung verlagert werden. Eine Verlagerung der Kompetenzen bedeutet, dass auch die Entscheidungsbefugnisse aus dem ehemaligen Zuständigkeitsbereich in den neuen wandern. Datentransfer ist in der Regel eine Beschneidung derjenigen Abteilung, die zuvor die Daten verwaltet und bearbeitet hat. Weiterbildung wird so zentral gesteuert, statt zwischen MitarbeiterIn und Vorgesetztem/r vereinbart, Personalrekruiting erfolgt über zentrales Ranking von Kandidatinnen, etc.. So gehen auch mittleren und höheren Managementebenen Macht und Einfluss verloren. Diese werden an eine übergeordnete zentrale Einheit übergeben.

**mehr Verantwortung**

Geraten **Daten in die falschen Hände**, hat das weit reichende Folgen für die Verantwortlichen. Auch wenn der Missbrauch aus Gründen passiert ist, die die Führungskraft nicht beeinflussen kann, weil sie außerhalb ihres Zuständigkeitsbereichs liegen, hat sie eine Verantwortung für die rechtmäßige Verwendung der übermittelten Daten.

Auch durch missbräuchliches Verhalten der Führungskräfte können Straftaten entstehen. Verschafft sich beispielsweise eine Führungskraft ohne Zustimmung der Betroffenen und ohne Legitimation durch eine Betriebsvereinbarung Zutritt zu sensiblen Daten von MitarbeiterInnen, kann sich das in einer **Geldstrafe** von bis zu 18.890 EUR auswirken (§ 52 DSG, siehe auch Kapitel 7.1.1).

**Beispiel aus der Praxis eines internationalen Transportunternehmens**
Vor zwei Jahren sollten umfangreiche Datenbestände über die MitarbeiterInnen in die Konzernzentrale in den Niederlanden gesendet werden. In einer europäischen Betriebsratssitzung haben die BetriebsrätInnen dem CEO klargemacht, dass er persönlich vom Euro-Betriebsrat verklagt werden würde, wenn Daten im Rahmen der SAP-Verwaltung missbräuchlich verwendet werden. Dieses Vorhaben wurde ausschließlich mündlich, ohne offizielles schriftliches Dokument mitgeteilt. Nur im Meeting-Protokoll wurde das Vorhaben vermerkt. Seitdem merkt man im Unternehmen einen vorsichtigeren Umgang, wenn es um Daten geht, so werden z.B. keine Privatadressen von MitarbeiterInnen aus Deutschland und Österreich an das Headoffice weitergegeben. Das kann auch daran liegen, dass bei solchen "Nebensächlichkeiten" die Gefahr als Unternehmen in der Öffentlichkeit zu stehen, zu hoch eingeschätzt wird. Alle Informationen über einzelne MitarbeiterInnen (Lohn, Arbeitszeit, Produktivität, u.s.w.) verbleiben derzeit im Land und werden nur als anonymisierte Gesamtinformation weitergegeben.

**Konkurrenz belebt das Geschäft?**

Nicht nur die MitarbeiterInnen auf den niedrigeren Hierarchieebenen sind durch die zentrale Speicherung und Verknüpfung ihrer Daten einen **verstärkten Wettbewerb** unterworfen. Dasselbe gilt auch für den Managementbereich. Sowohl die quantitative als auch die qualitative Performance wird gerankt und das erzeugt in der Regel einen starken Druck - insbesondere wo einheitliche Kriterien quer über alle Firmenkulturen und länderspezifischen Traditionen drüber gelegt werden.

**Arbeitsaufwand**

Außerdem bringt eine zentrale Verarbeitung von Daten selten jene versprochenen Kosteneinsparungen und Synergieeffekte. Nachdem die zentralen Datenverarbeitungseinheiten mit den nationalen Gebräuchen in den seltensten Fällen vertraut sind, muss nicht nur das technische System vereinheitlicht werden, sondern es sind auch unzählige Informationen einzuholen und von den nationalen Standorten zu liefern. Der Raum für Missverständnisse ist groß. Einmal unterlaufene Fehler müssen in mühevoller Kleinarbeit über mehrere Etappen hinweg zurück verfolgt werden. Denn je mehr Personen an einem System sitzen, desto fehleranfälliger wird die Datenverarbeitung. **Je weiter weg vom Geschehen die Datenverarbeitung erfolgt, desto länger sind die Bearbeitungswege** - auch wenn es sich dabei um elektronische und virtuelle Wege handelt.

**Kosten**

Zum Thema Finanzen kommt auch oft das Argument, dass die Sicherheit der MitarbeiterInnen-Daten zu umständlich, technisch höchst schwierig und damit viel zu teuer wäre. Wenn die Daten allerdings ungeschützt in der ganzen Welt zirkulieren, entstehen materielle Schäden und Kosten durch den Arbeitsaufwand, strafrechtliche Schäden für die missbräuchliche Verwendung der Daten und Imageschäden. Mittelfristig bewirkt ein effizientes Sicherheitsmanagement Kosteneinsparungen.

Einige Konzerne haben ihre Zentralisierungsversuche bereits wieder rückgängig gemacht. Der Aufwand rechnete sich nicht. Um diesem „Hin-und-Her“ zuvor zu kommen, wäre ein Überdenken der Datentransfers im Vorhinein äußerst sinnvoll.

**Beispiel aus der Praxis eines europaweiten Versicherungsunternehmen**
Das Servicecenter für Kundenanfragen wurde konzernweit zentralisiert und nach Indien verlagert. Die KundInnen sind bei den kleinsten Anfragen z.B. auf deutsch, englisch, spanisch, etc. mit perfekt die jeweilige Sprache beherrschenden InderInnen konfrontiert gewesen. Allerdings haben es diese aufgrund der sozialen und kulturellen Unterschiede oft nicht geschafft, die Sachverhalte von Schadenfällen einwandfrei aufzunehmen und Erstveranlassungen zu treffen (z.B. bei einem Wasserleitungsgebrechen ist das Wort für Ablaufgully in Österreich ein anderes in der Schweiz oder Norddeutschland. Ein Anspruch auf einen Mietwagen hat in Österreich einen anderen Namen als in Deutschland oder der Schweiz.) Durch Häufung der Fehlveranlassungen der indischen MitarbeiterInnen und durch massive Beschwerden vor allem der schweizerischen und deutschen KundInnen musste die Auslagerung dieses Servicecenters binnen kürzester Zeit rückgängig gemacht werden.
Die Hinweise der lokalen Betriebsräte auf mögliche Probleme mit KundInnen wurden vor der Auslagerung mit Wirtschaftlichkeits- und Rationalisierungsargumenten zurück gewiesen. Die nachfolgenden Berechnungen der deutschen und schweizerischen Betriebsräte zu den verursachten unnötigen Kosten durch die Auslagerung und die von ihnen dokumentierten vorangehenden Hinweise an die Geschäftsleitung (Gesprächsprotokolle mit Unterschriften der anwesenden Personen) haben auch zu einem Wechsel in der Geschäftsleitung geführt, lokale MitarbeiterInnen wurden wieder eingestellt.


**schriftliche Protokollierung**

**Machen Sie's schriftlich!** Die **Dokumentation** der Ereignisse im Zuge von Ausgliederungen (z.B. Gesprächsprotokolle von Treffen mit der Geschäftsleitung) erleichtert die nachfolgenden Verhandlungen. Ein Monitoring durch den/die Betriebsrat/rätin verspricht mitunter Erfolg. „Dokumentiere bei Zeiten, dann hast du in der Not." - rät auch das deutsche Bundesamt für Sicherheit in der Informationstechnik.

Das selbe gilt für Protokolle zu technischen und organisatorischen Maßnahmen der Datensicherheit. Aber übertreiben sie die Protokollflut nicht! Protokolliert im Sinne des DSG muss nur dann werden, wenn dem Missbrauch personenbezogener Daten vorgebeugt werden muss, die **im Verantwortungsbereich der Firma/des Konzerns** liegen[8]. Werden die Protokolle über Schritte der Datensicherung zur Kontrolle der MitarbeiterInnen verwendet - schlecht, weil das ist unzulässig!

**Kundenzufriedenheit durch Datenschutz**

Ein guter innerbetrieblicher Datenschutz stärkt das Vertrauen und damit die Loyalität der MitarbeiterInnen. Vertrauen und Loyalität sind motivations- und damit auch leistungsfördernde Komponenten des Arbeitsalltags. Ein gutes Sicherheitsmanagement verstärkt die Identifikation der MitarbeiterInnen mit dem Unternehmen. Ein Unternehmen, das verantwortungsvoll mit den Daten der MitarbeiterInnen umgeht, kann auch glaubwürdig darstellen, dass es mit KundInnen-Daten ebenso verantwortungsvoll umgeht. Nachgewiesene Sicherheit im Bezug auf MitarbeiterInnen-Daten wirkt sich auch auf die Beziehung der MitarbeiterInnen zu den KundInnen aus. **Die Attraktivität eines Unternehmens für KundInnen und GeschäftspartnerInnen steigt mit dessen Datensicherheit.**

**gemeinsames Handeln**

Wie die eben beschriebenen Argumente deutlich gemacht haben, sind Datenschutzmissbräuche für das Management mindestens genau so unangenehm, wie für MitarbeiterInnen. **Mittleres und höheres Management sollte ins Boot geholt werden.** Das stärkt die ArbeitnehmerInnenvertretung bei innerbetrieblichen Verhandlungen zu klaren Datenschutz-Regelungen.

[8] Das Unternehmen hat keine Pflicht, den Zugriff auf unternehmensfremde, illegale Seiten zu verhindern. Daher muss auch nicht jeder Internet-Besuch protokolliert werden.

## 9.3 SystemadministratorInnen - sie sehen alles!

**zwiespältige Aufgaben**

SystemadministratorInnen haben Zugriff auf so gut wie alle Daten, die einE MitarbeiterIn hinterlässt, selbst produziert oder sich auch nur anschaut. SystemadministratorInnen unterliegen der Verschwiegenheitspflicht. Diese Pflicht trifft sowohl unternehmensinterne Daten als auch persönliche Daten der MitarbeiterInnen. Nun zeigt sich in der Praxis aber häufig, dass es die Geschäftsführung mit der Einsichtnahme in persönliche Daten nicht allzu genau nimmt und von dem/der SystemadministratorIn auch ohne Anlassfall und Begründung Einsicht verlangt. Der/die SystemadministratorIn sitzt in der Klemme - handelt er/sie nach den Anweisungen des/der Chefs/-in oder widersetzt er/sie sich diesen und handelt gemäß österreichischer und europäischer Gesetzeslage.

**klare Vereinbarungen**

Um derartige Konfliktsituationen zu vermeiden, wäre es sinnvoll, fixe Rahmenbedingungen für genau diese Situationen zu schaffen. Dort ist klar angeführt, dass nur auf ausdrückliches Verlangen der Geschäftsführung die Einsicht in persönliche Daten gewährt wird. Dazu braucht es in der Regel konkrete Verdachtsmomente. Damit ist der Eingriff nachvollziehbar und kann gegebenenfalls von Datenschutzbeauftragten/dem Betriebsrat kontrolliert werden.

## 9.4 Europäischer/Welt-Betriebsrat - sie agieren grenzenlos

**Sprachbarrieren**

Eine große Schwierigkeit in der internationalen Betriebsratsarbeit besteht darin, Begriffe, die sich aus einer bestimmten nationalen Perspektive ergeben, so zu fassen, dass sie auch in anderen Sprachen und Traditionen verstanden werden können. Z. B. haben Sozialdaten unterschiedliche nationale arbeitsrechtliche Hintergründe und führen daher zu unterschiedlichen Begrifflichkeiten und Definitionen. Aber auch gleich lautende Bezeichnungen haben oftmals unterschiedliche Bedeutungen. Eine Arbeitsgruppe sollte daher abklären ob die Begriffe international unterschiedliche Bedeutungen haben.

**Erfahrungsbericht aus einem Versicherungskonzern**

Das Unternehmen wollte bestimmte Geschäftsbereiche auslagern. Dazu suchte das Managementteam nach Gründen, die belegen sollten, weshalb die europäischen MitarbeiterInnen schlechter qualifiziert wären, als die potentiellen MitarbeiterInnen in einem angestrebten Zielland der Dritten Welt. Die mangelnde Sprachkompetenz sollte als Argument herhalten. Nachdem dies bei einem Meeting des globalen Managementteams mit den obersten Europäischen Betriebsräten kommuniziert wurde, hatten einige Betriebsräte die Idee, dass durch eine anonyme Befragung in Österreich und Italien die Sprachkompetenz erhoben werden sollte. Nicht bedacht wurde dabei, dass viele ÖsterreicherInnen multikulturelle Hintergründe hatten, aber auch viele Italiener konnten Sprachkompetenz vorweisen. Das Ergebnis war so positiv, dass diese MitarbeiterInnen - ohne, dass diese es wahrgenommen hätten - einen Beitrag zur Verhinderung des Outsourcing geliefert haben. Erst später durften die involvierten Betriebsräte davon berichten. Übrigens hatten diese Betriebsräte dem Management vorgeschlagen, als nächstes in der Schweiz eine anonyme Befragung durchzuführen.

**Konzernvereinbarungen**

In international agierenden Konzernen reicht es nicht aus, Betriebsvereinbarungen mit der österreichischen Geschäftsführung zu vereinbaren. Denn die nationalen Vereinbarungen kümmern die internationale Geschäftsführung erfahrungsgemäß wenig. Dagegen hilft eine Konzernvereinbarung, die die Datentransfers von der österreichischen Tochtergesellschaft an die Konzernmutter klar regelt.

**Erfahrungsbericht eines internationalen Pharmakonzerns**

Im ersten Quartal 2006 wurde der Konzernbetriebsrat darüber informiert, dass geplant ist, weltweit ein Personalinformationssystem auszurollen. Dieses System soll in standardisierter Form Personaldaten erfassen, verwalten und verarbeiten.

45 Personalinformationen pro Mitarbeiter und Mitarbeiterin werden in diesem System erfasst. Einzelne Daten aus diesem System werden in weiterer Folge an Drittsysteme im Konzern weitergegeben.

Die Einführung dieses Systems hat zum Ziel:

- durch harmonisierte Datenbeschreibungen über System- und organisatorische Grenzen hinweg vergleichbare Informationen zur Belegschaft zu erhalten;
- schnell und effizient regionale und globale Übersichten über die Belegschaft und deren Entwicklung zu erhalten;
- durch eine global gültige Personalidentifikationsnummer MitarbeiterInnen über System- und organisatorische Grenzen hinweg eindeutig identifizieren zu können;
- die lokale Administration der MitarbeiterInnen und die Personalführungsprozesse zu unterstützen;
- durch die Übermittlung von Basispersonaldaten aus dem Personalinformationssystem die Konsistenz von MitarbeiterInnendaten in IT-Systemen zu verbessern sowie die Datenverwaltungsprozesse in diesen IT-Systemen zu vereinfachen.

Nachdem der Betriebsrat alle verfügbaren Informationen des Systems durch Arbeiterkammer und Gewerkschaft prüfen ließ, wurde beschlossen eine Konzernbetriebsvereinbarung über die Erfassung, Übermittlung und Verarbeitung von personenbezogenen Daten abzuschließen.

Einige der 45 Datenfelder bezogen sich auf die Leistungsdaten der MitarbeiterInnen. Es war das Ziel des Konzernbetriebsrates diese Informationen in jedem Fall zu schützen und einen Transfer in die Konzernzentrale zu verhindern.

Mit der Erfassung, Verarbeitung und Übermittlung von Performancedaten kann der Konzern sehr einfach Leistungsvergleiche einzelner Standorte, Bereiche und MitarbeiterInnengruppen über die Ländergrenzen hinweg vornehmen, deren Auswirkungen im schlimmsten Fall von Reorganisationen bis Standortschließungen/-verlagerungen reichen können. Diese Gefahr wollte der Konzernbetriebsrat von den österreichischen Standorten abwenden und hat alle Anstrengungen unternommen, den Transfer dieser Daten abzuwenden. Zunächst wurden die Beschäftigten im Rahmen von Betriebsversammlungen über die Absichten des Unternehmens informiert und über mögliche arbeitsrechtliche und strukturelle Konsequenzen aufmerksam gemacht. Danach wurden mit Unterstützung von Arbeit & Technik der GPA-djp die Verhandlungen mit dem Management aufgenommen. Nach mehreren schwierigen Verhandlungsrunden konnte eine Konzernbetriebsvereinbarung abgeschlossen werden.

In dieser Betriebsvereinbarung wurden die Verwendungsgrundsätze verankert:

- Umfang der Datensammlung,
- Umfang der Datenverarbeitung,
- Frequenz der Datenaktualisierung,
- Weitergabe an Drittsysteme,
- Weitergabe von Daten via Reports über die Landesgrenzen hinweg,
- Zugriffsbeschränkungen,
- Trainings,
- Dauer der Aufbewahrung,
- Rechte der MitarbeiterInnen und die
- Kontrollrechte des Betriebsrates.

Zudem ist es gelungen, die Weiterleitung und Verarbeitung von Performancedaten und alle Informationen die damit im Zusammenhang stehen auszuschließen.

Ein Jahr nach Einführung des Systems hat der Konzern bereits Auswertungen und Gegenüberstellungen von Daten - mit Ausnahme von Österreich - über die MitarbeiterInnen-Performance der einzelnen Divisionen und Ländern vorgestellt.

Aus österreichischer Sicht haben sich die Anstrengungen des Konzernbetriebsrates, Leistungsdaten aus der Betriebsvereinbarung herauszuverhandeln, jedenfalls gelohnt.

**nationale Unterschiede in der Rechtslage**

In einigen Ländern sind Konzernbetriebsvereinbarungen in der nationalen Gesetzgebung nicht vorgesehen. Der Europäische Betriebsrat muss sich daher je nach Länderspezifika eine geeignete Vorgangsweise überlegen. In Frankreich beispielsweise hat der oben erwähnte Pharmakonzern einen privatrechtlichen Vertrag mit der nationalen Konzernleitung, der sicherstellt, dass persönliche Daten nicht zum Nachteil der Belegschaft verwendet werden.

**andere KonzernbetriebsrätInnen als Verbündete**

Auf länderübergreifender Ebene geht es vor allem darum, sich BündnispartnerInnen zu suchen. Wie genau die Datenschutzvereinbarungen aussehen, ist nationaler Gesetzgebung unterworfen, aber dass Konzernweite Vereinbarungen mit ähnlichem Inhalt bestehen, stärkt die Belegschaft und schützt ihre Daten. So können sie nicht gegeneinander ausgespielt werden.

# 10) Gewerkschaftliche Forderungen zum Datenschutz

**Sensibilisierung der Öffentlichkeit**

Nicht nur auf betrieblicher Ebene sondern auch auf gesamtgesellschaftlicher Ebene ist es an der Zeit, Datenschutzangelegenheiten mehr Aufmerksamkeit zu widmen. Wird das Thema in einer breiteren Öffentlichkeit diskutiert, wächst das Bewusstsein für die dahinter stehenden Probleme und es kann gemeinsam mehr öffentlicher Druck auf politischer Ebene erzeugt werden.

**gesetzliche Maßnahmen**

Die GPA-djp fordert die gesetzliche Verankerung einer/s unabhängigen betrieblichen Datenschutzbeauftragten (DSB) auf Grundlage der nationalen Gesetzgebung und/oder der EU-Gesetzgebung.

**Anforderungen an eineN DatenschutzbeauftragteN:**

Unternehmen, die personenbezogene Daten automatisiert bzw. auf einem anderen Weg erheben, verarbeiten oder nutzen, haben ab einer bestimmten (noch zu definierenden) Anzahl von Beschäftigten (einschließlich Teilzeitkräfte, freier MitarbeiterInnen, Leiharbeitskräfte) eineN betrieblicheN DSB zu installieren.

DSB sind in der Ausübung der ihr übertragenen Aufgaben weisungsfrei. Gegenüber den Organen der Belegschaftsvertretung ist der/die DSB zur Information verpflichtet.

Die Bestellung bzw. die Auswahl des/der DSB bedarf der Zustimmung der zuständigen Belegschaftsorgane. Dies gilt auch dann, wenn ein Betriebsratsmitglied die Aufgaben des/der DSB übernimmt.

Dem/der DSB dürfen im Zuge der übertragenen Tätigkeit keine Benachteiligungen entstehen, insbesondere hinsichtlich des Entgelts, der Aufstiegsmöglichkeiten und der Versetzung.

DSB nehmen durch die Ausübung ihrer Aufgaben die Position einer/s SpezialistIn ein. In Konsequenz sind entsprechende kollektivvertragliche Einstufungen zu berücksichtigen.

DSB sind vor einer im Zusammenhang mit ihrer Tätigkeit stehenden Kündigung bzw. Entlassung zu schützen.

Die Verantwortung für die Einhaltung des Datenschutzes entsprechend aller gesetzlichen Bestimmungen liegt beim/bei der ArbeitgeberIn. Der/die DSB ist im Zusammenhang mit seiner/ihrer Tätigkeit schad- und klaglos zu halten. Es sei denn, er/sie handelt vorsätzlich oder grob fahrlässig.

ArbeitgeberInnen haben den/die DSB bei ihrer Tätigkeit zu unterstützen. Das bedeutet insbesondere die Bereitstellung aller für die Tätigkeit erforderlichen Mittel, Geräte, Räume, Hilfspersonal sowie die Gewährung der erforderlichen Zeit unter Fortzahlung des Entgeltes.

Als DSB können nur Personen bestellt werden, die entsprechende Fachkompetenz (Ausbildung) nachweisen können. Die Kostenübernahme von Aus- und Weiterbildung für Datenschutzbeauftragte ist von ArbeitgeberInnenseite zu übernehmen.

Für die Ausbildungszeit ist der/die DSB von der Arbeitsleistung unter Fortzahlung des Entgeltes freizustellen. Eine Vereinbarung gemäß § 2 d des AVRAG, wonach Entgelt und/oder Ausbildungskosten von dem/der DSB rückgefordert werden können, ist unzulässig.

Dem/der DSB ist unaufgefordert eine Übersicht über die Dateien und über die Datenverarbeitungsanlagen sowie auch die Versions-Änderung von Verfahren/Prozessen bereit zu stellen.

Die im Zuge der Einsetzung bzw. der Tätigkeit von DSB entstehenden Kosten werden von ArbeitgeberInnenseite getragen.

Mit den Aufgaben einer/s DSB können auch unternehmensexterne Personen betraut werden. Entsprechende Vertraulichkeitsverpflichtung ist sicherzustellen.

Eine gesetzliche Verankerung betreffend DSB ist im Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz) vorzunehmen. Die als DSB bestellten Personen sind beim Datenverarbeitungsregister zu melden.

**Aufgaben des/der Datenschutzbeauftragten:**

Die nachfolgenden Aufgaben beschreiben schwerpunktmäßig jene Aufgaben, die sich aus dem Fokus der Verarbeitung von MitarbeiterInnendaten ergeben. Darüber hinaus gibt es auch Aufgabenstellungen zur Regelung der Erfassung und Verarbeitung von KundInnen- bzw. LieferantInnendaten, die hier nicht im einzelnen aufgeführt werden, aber dennoch im Aufgabenbereich des/der DSB liegen. Gegebenenfalls bedarf es besonderer Regelungen, wenn KundInnen gleichzeitig auch MitarbeiterInnen sind:

- Der/die DSB unterstützt, informiert und berät den/die ArbeitgeberIn bei der Wahrnehmung seiner/ihrer Verantwortung zur Sicherstellung des betrieblichen Datenschutzes.

- Der/die DSB ist fachkundigeR AnsprechpartnerIn der Belegschaft bzw. den Organen der Belegschaftsvertretung in allen Belangen des betrieblichen Datenschutzes und auskunftsberechtigt gegenüber diesen.

- Der/die DSB trägt insbesondere Sorge für die Einhaltung aller gesetzlichen Bestimmungen zum betrieblichen Datenschutz. Dabei überwacht er/sie die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen, die in Verbindung mit personenbezogenen Daten stehen.

- Der/die DSB informiert, sensibilisiert und schult die Belegschaft, insbesondere die mit der Verarbeitung von personenbezogenen Daten beschäftigte Personen sowie die Organe der Belegschaftsvertretung in Belangen des betrieblichen Datenschutzes.

- Der/die DSB ist bei der Planung und Einführung neuer Technologien der Datenverarbeitung im Betrieb zu Rate zu ziehen.

- Kommt es zu einer Auslagerung von Datenerhebungen bzw. der Datenverarbeitung, trägt der/die DSB des auslagernden Unternehmens Sorge, dass nur jene Daten ausgelagert werden, die im Sinne des Datenschutzes tatsächlich auslagerbar sind. Darüber hinaus hat der/die DSB das Recht und die Pflicht, im Unternehmen, in das ausgelagert wurde, die Einhaltung des Datenschutzes zu kontrollieren. Das Unternehmen, in das ausgelagert wurde, ist verpflichtet, dem/der DSB des auslagernden Unternehmens alle erforderlichen Informationen zu erteilen und Einsichtnahmen zu ermöglichen. Anfallende Kosten gehen zu Lasten des auslagernden Unternehmens.

# 11) Schlusswort

Beim Schutz von MitarbeiterInnen-Daten vor unerwünschtem Zugriff spielen mehrere Faktoren eine wesentliche Rolle. Es müssen **rechtliche, technische und organisatorische Maßnahmen** getroffen werden, um in einem optimalen, auf die jeweilige Situation abgestimmten Zusammenspiel den Schutz der MitarbeiterInnen vor missbräuchlicher Verwendung ihrer Daten zu gewährleisten.

Dazu ist eine **Zusammenarbeit** von Betriebsrat, Beschäftigten und Geschäftsführung notwendig. Der Betriebsrat hat dabei die Schlüsselfunktion. Ihm werden die Systeme zur Datenanwendung von der Geschäftsführung vorgestellt, bei ihm laufen die Informationen zusammen, an ihn wenden sich sensibilisierte MitarbeiterInnen mit ihren Bedenken, er holt sich Unterstützung bei der Gewerkschaft zu diesem komplexen Thema. Die Gewerkschaft leistet Beratungsarbeit. Die MitarbeiterInnen machen auf Missstände aufmerksam und geben Rückendeckung. Vielleicht kann man manchmal die Geschäftsführung mit ins Boot holen um gegen den Konzernstrom zu rudern. Aber auf die Füße stellen müssen sich die BetriebsrätInnen selbst. Je größer das Netzwerk an Verbündeten ist das sie dabei hinter sich haben (z.B. System-AdministratorInnen, Euro-BetriebsrätInnen, Gewerkschaft, etc.) desto mehr Aussicht auf Erfolg haben sie.

**Generell gilt für Vereinbarungen zum Datenschutz:**

- **Je mehr der/die EmpfängerIn der Daten in deren Verwendung beschränkt ist, desto mehr Sicherheit haben die Betroffenen.**
- **Je höher die Verantwortung für alle Vorgänge im Zusammenhang mit dem Datentransfer für die AuftraggeberInnen ist, desto mehr Sicherheit haben die Betroffenen.**


# Anhang

## Wichtiges im Internet

### Österreich:

GPA-djp (Arbeit und Technik) **Muster-BV Rahmenbedingungen:** http://www.gpa-djp.at ➜ Arbeitsgestaltung ➜ Arbeitsorganisation ➜ Betriebsvereinbarungen im Überblick ➜ Daten

GPA-djp (Arbeit und Technik) **Muster-BV SAP:** http://www.gpa-djp.at ➜ Arbeitsgestaltung ➜ Arbeitsorganisation ➜ Betriebsvereinbarungen im Überblick ➜ SAP

GPA-djp (Arbeit und Technik) in Zusammenarbeit mit der Juristin Souhrada-Kirchmayer vom Verfassungsdienst des Bundeskanzleramtes (2004): **„Das Datenschutzgesetz aus Sicht der ArbeitnehmerInnen"** - Download ist erhältlich unter: http://www.gpa-djp.at ➜ Arbeitsgestaltung ➜ Arbeitsorganisation ➜ Broschüren im Überblick ➜ Datenschutzgesetz

GPA-djp (work@IT) (2007): **„Rächer der enterbten Daten" -** Download unter http://www.gpa-djp.at ➜ Interessensvertretung ➜ work@IT ➜ Datenschutz und Security

Die **ARGE Daten** bietet auf ihrer Homepage aktuellen News zum Thema Datenschutz allgemein, Rechtsinformationen und Zertifizierungen zur Datensicherheit. Die ARGE-Daten bietet die derzeit österreichweit einzige überbetriebliche Ausbildung zu Datenschutzbeauftragten an: http://www.argedaten.at/

Die **Datenschutzkommission** findet man unter der Adresse: http://www.dsk.gv.at/

Das **Datenschutzgesetz**:http://www.dsk.gv.at/dsg2000d.htm

Bundeskanzleramt (2007): **„Das Österreichische Informationssicherheitshandbuch"** enthält alle wesentlichen Schritte, die erforderlich sind um ein innerbetriebliches Sicherheitsmanagement zu betreiben. Zielgruppen sind sowohl die Privatwirtschaft als auch mittlere und größere Organisationen - für die öffentliche Verwaltung ist es per Ministerratsbeschluss vom Juli 2007 explizit empfohlen: http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=23263

Arbeiterkammer Wien - KonsumentInnenschutz (2002): **„Datenschutz"** - Download unter: http://www.arbeiterkammer.at/pictures/importiert/Datenschutz.pdf

Die **Rechtsanwaltskanzlei** Preslmayr und Partner hat sich unter anderem auf den Bereich Datenschutz spezialisiert und berät auch ArbeitnehmervertreterInnen.
http://www.preslmayr.at/
http://www.preslmayr.at/frame_dt/site_dt/text_d_datenschutz.htm

### Europa:

Richtlinien, Rechtssprechung, Standardvertragsklauseln, nationale Kontaktadressen, etc. der **EU-Kommission**: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

Das Formular der EU-Kommission zu den **Standardvertragsklauseln**:
http://eur-lex.europa.eu/LexUriServ/site/de/oj/2004/l_385/l_38520041229de00740084.pdf

Vorschlag der **EU- Datenschutzgruppe**, wie **verbindliche unternehmensinterne Regelungen** aussehen sollten:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_de.pdf

Artikel 29 Datenschutzgruppe (2001): **Stellungnahme der Artikel 29 Datenschutzgruppe zur Verarbeitung personenbezogener Daten von Beschäftigten.**
Diese Stellungnahme ist eine rechtliche Empfehlung, sie schafft keine rechtliche Verbindlichkeit.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48de.pdf

Frank Hendrickx (2002): **"Protection of workers' personal data in the European Union"**:
http://ec.europa.eu/employment_social/labour_law/docs/dataprotection_hendrickx_combinedstudies_en.pdf
Für den internationalen Vergleich ist diese englischsprachige Werk gut geeignet.

Arbeiterkammer Saarland (Hg.) (2004): **„Datenschutz im Arbeitsverhältnis, ein Handlungsratgeber für Betriebsräte, Personalräte, Mitarbeitervertretungen, Arbeitnehmerinnen und Arbeitnehmer zu Bestimmungen des Datenschutzes."**
Saarbrücken: http://www.fh-giessen-friedberg.de/datenschutz/content/view/28/13/

Das **deutsche Bundesamt für Sicherheit in der Informationstechnik**
bietet umfangreiche Informationen - auch als Download - zum IT-Grundschutz:
http://www.bsi.bund.de/gshb/index.htm

## Weltweit:

Die **us-amerikanischen Safe-Harbor**-Bestimmungen des Handelsministeriums sowie die jeweils aktuellen Firmen, die sich Safe-Harbor unterworfen haben findet man unter:
http://www.export.gov/safeharbor/

Der Code der **Internationalen Arbeitsorganisation (ILO)** zum Schutz von ArbeitnehmerInnen-Daten. Auch wenn der Vorschlag der ILO aus dem Jahr 1997 stammt, enthält die englisch sprachige Publikation nach wie vor aktuelle Hinweise:
http://www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf

Der von der OECD entwickelte **„OECD-Privacy Policy Generator"** steht zur Verfügung:
http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html

# Literatur

Ghali Ivonne (1999): „**Datenschutz Rechtsgrundlagen**, Kurzkommentar, Darstellung der Verfahren, Stand 1. Jänner 2000" WEKA-Verlag. Wien. Kommentiertes Datenschutzgesetz plus Datenschutzrelevante Rechtsmaterien in anderen Gesetzestexten.

Knyrim Rainer (2003): „**Praxishandbuch Datenschutzrecht** - Leitfaden für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm." Verlag Manz . Kommentiertes Datenschutzgesetz aus Unternehmenssicht mit vielen Praxisbeispielen

# Glossar

**Angemessenes Schutzniveau**
Das „angemessene Schutzniveau" besteht dann, wenn in einem Land rechtliche Rahmenbedingungen (z.B. ausführliches Gesetz) und institutionelle Rahmenbedingungen (z.B. Kommission für Einsprüche) gegeben sind, die den Datenschutz festlegen. Die EU prüft und bestimmt, wann ein „angemessenes Schutzniveau" in einem Land besteht. Derzeit besteht ein „angemessenes Schutzniveau" in allen EU-Länder, Schweiz, Liechtenstein, Norwegen, Island, den Kanalinseln Guernsey und Isle of Man, Kanada, Argentinien und Australien.

**AuftraggeberInnen**
Ist die Person oder das Unternehmen, die Daten verarbeiten bzw. den Auftrag zur Datenverarbeitung an Dritte erteilen.

**Bereichsbezogene oder bereichsspezifische Personenkennzeichen**
Sind jene Zahlen- und/oder Buchstabenkombinationen, die (meist von einer Behörde oder einer großen Firma) für Einzelpersonen vergeben werden (z.B. Kundennummer, Sozialversicherungsnummer). Das personenbezogene Kennzeichen kann nur von denen, die es vergeben haben, einer konkreten Person zugeordnet werden. Die Verwendung ist nur für die eine Anwendung, für die sie erfunden wurden, zulässig.

**Data Mining**
Von Data Mining wird gesprochen wenn riesige Datenmengen mittels hoch komplexer statistisch-mathematischer Verfahren untersucht werden. Ziel dabei ist es, Gesetzmäßigkeiten in den riesigen Datensätzen aufzuspüren (z.B. Profile von KundInnen, Verhaltensprofile von MitarbeiterInnen,…).

**Data Warehouse**
Als Data Warehouse bezeichnet man die Ansammlung von unzähligen Daten (meist KundInnendaten). Die Daten werden in großen Datenbanken meist einzig zu dem Zweck gesammelt, um damit beliebige Verknüpfungen Berechnungen etc. durchführen zu können. Ein solches Vorgehen ist nach dem österreichischen Datenschutzgesetzt verboten.

**Datenanwendung**
früher hieß dieser Begriff „Datenverarbeitung". Man versteht darunter alle logisch miteinander verbundenen Schritte, die - zumindest teilweise - automationsunterstützt erfolgen um personenbezogene Daten für einen bestimmten Zweck zu gebrauchen. Eine Firma kann beispielsweise, die Datenanwendung "Personalverwaltung" führen. Es macht keinen Unterschied, ob dazu ein Softwarepaket für die gesamte Personalverwaltung verwendet wird oder ob getrennte Programme für Lohnbuchhaltung und Zeitverwaltung eingesetzt werden.

**Datenschutzkommission**
Die Datenschutzkommission im Bundeskanzleramt verwaltet das Datenverarbeitungsregister, prüft Ansuchen um Datenübermittlungen und -überlassungen und überprüft bei begründetem Verdacht Beschwerden von Betroffenen.

**Datenverarbeitungsregister**
Dieses Register wird von der Datenschutzkommission geführt und enthält alle Angaben darüber welche Unternehmen, welche Datenanwendungen benutzen.

**Datenverwendung**
Eine Datenverwendung ist jegliches Umgehen mit Daten. Verarbeiten, Ermitteln, Übermitteln und Überlassen fallen darunter.

**DienstleisterInnen**
Sind jene Unternehmen, die die Daten „verwenden", wobei mit „verwenden" jede Art der Datenhandhabung gemeint ist, sowohl das Verarbeiten als auch das Übermitteln von Daten ist damit gemeint.

**Dritte**
werden in der Datenschutzrichtlinie der EU definiert als diejenigen, welche zusätzlich zu den HauptakteurInnen für die Datenverarbeitung verantwortlich sind, also neben denen, auf die sich die Daten beziehen (Betroffene), denen, die die Datenanwendung in Auftrag geben (Auftraggeber) und denen, die die Daten verarbeiten. In der Regel werden sie dazu beauftragt. Es kann sich um reale Personen, Dienstleister, Firmen, Behörden u.a. juristische Personen handeln.

**E-Signatur**
Mit einer E-Signatur werden Dokumente unterzeichnet um ihre Echtheit zu garantieren. Nachdem eine graphische Unterschrift (z.B. im Attachment) keinen Rückschluss auf den/die tatsächliche VerfasserIn ermöglicht, werden E-Signaturen von Unternehmen entwickelt um sicher zu stellen, dass Dokumente wirklich von denjenigen kommen, die vorgeben, sie zu schicken.

**Empfänger**
Sind alle juristischen Personen, die Daten erhalten (z.B. Unternehmen, Behörden, Dritte,…).

**Ermitteln von Daten**
Dabei werden Daten erhoben um sie später in einer Datenanwendung weiter zu verwenden.

**Informationsverbundsystem**
Besteht, wenn mehrere Auftraggeber (z.B. innerhalb eines Konzerns) Daten gemeinsam benutzen.

**Löschen von Daten**
Darunter versteht man das unkenntlich machen von Daten.

**Meldepflicht**
Jede Datenanwendung muss bevor sie in Betrieb geht, bei der Datenschutzkommission gemeldet werden - und zwar vom Auftraggeber. Es gibt verschiedene Ausnahmen von der Meldepflicht.

**Musterverordnung**
In der Standard- und Musterverordnung ist von dem/der BundeskanzlerIn festgelegt, welche Daten für welche Datenanwendungen gemeldet werden müssen.

**Personenbezogene Daten**
Sind jene Daten, die einen eindeutigen Rückschluss auf eine bestimmte Person zulassen. Dazu zählen z.B. alle biometrischen Daten (Größe, Gewicht, Haarfarbe, Fingerabdruck,..), Sozialversicherungsnummer, Adresse etc. Ob ein Datum personenbezogen ist, kann man oft erst an der Verknüpfung von Daten erkennen. Die Haarfarbe alleine sagt z.B. noch nichts aus, aber kombiniert mit Ausbildung, Berufsbezeichnung und Einkommen lassen sich vielleicht schon eindeutige Rückschlüsse auf eine Person ziehen.

**Safe Habor**
Bei den Safe-Harbor-Richtlinien handelt es sich um us-amerikanische Vereinbarungen, die den EU-Richtlinien zum Datenschutz weitgehend entsprechen. Us-amerikanische Unternehmen, die sich den Safe-Harbor-Richtlinien unterwerfen, haben per EU-Beschluss „angemessenes" Datenschutzniveau, die Übertragung ist rechtlich zulässig.

**Sensible Daten**
Sind jene Daten, die über die personenbezogenen Stammdaten hinausgehen, also z.B. politische Zugehörigkeit, religiöses Bekenntnis, sexuelle Ausrichtung,…

**Sperren von Daten**
Damit werden Daten für die weitere Verwendung eingeschränkt. Vorab werden Daten meist gekennzeichnet um sie in weiterer Folge sperren zu können.

**Stammdaten**
Bleiben stabil, verändern sich im Laufe der Zeit kaum. Die Stammdaten einer Person umfassen z.B. Name, Geburtsdatum, Sozialversicherungsnummer, Adresse, Nationalität.

**Standardanwendungen**
Sind Datenanwendungen, die üblicher Weise für einen bestimmten Zweck benutzt werden und in der Regel keine sensiblen Daten betreffen, die schutzwürdigen Geheimhaltungsinteressen der Betroffenen also nicht gefährden. Sie werden per Verordnung des/der Bundeskanzlers/-in festgelegt (z.B. SA 002 BGBl. II Nr. 232/2003; Personalverwaltung für privatrechtliche Dienstverhältnisse). Darin ist von dem/der BundeskanzlerIn haargenau festgelegt, welche Datenerhebungen für welche Datenanwendungen auch ohne Meldung bei der Datenschutzkommission erlaubt sind. Diese Anwendungen sind weder genehmigungs- noch meldepflichtig.

**Standardvertragsklauseln**
Diese erleichtern den Datentransfer in Länder außerhalb der EU, die kein angemessenes Datenschutzniveau haben. Sie müssen zwischen den VertragspartnerInnen abgeschlossen werden und werden v.a. im internationalen Austausch von Steuer- und Zollbehörden verwendet. Die Datenschutzkommission muss den Datentransfer ins Datenverarbeitungsregister aufnehmen.

**Überlassung von Daten**
Das Unternehmen /der Dienstleister, dem die Daten überlassen werden, macht genau das selbe zum selben Zweck mit den selben Daten wie der Auftraggeber. Überlassung ins Nicht-EU-Ausland muss der DSK gemeldet werden.

**Übermittlung von Daten**
Dabei handelt es sich um die Weitergabe von ermittelten oder gespeicherten Daten an Dritte. Übermittlung ist die Verwendung von Daten für ein anderes Aufgabengebiet als der/die AuftraggeberIn ursprünglich vorgesehen hat (z.B. die Veröffentlichung von Daten). Von Übermittlung wird nicht gesprochen, wenn die Daten an den/die Betroffenen oder den/die AuftraggeberIn weitergegeben werden.

**Verarbeitung von Daten**
Unter diesen Begriff fällt das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten, etc. Also jegliche Handhabung von Daten - ausgenommen das Übermitteln von Daten.

**Vorabkontrolle**
Eine Vorabkontrolle ist eine Prüfung durch die Datenschutzkommission und wird von der DSK vorgenommen, wenn sensible Daten ins Ausland übermittelt werden sollen (z.B. strafrechtlich relevante Daten, Daten über die Kreditwürdigkeit einer Person).

**Zustimmung**
Eine Zustimmung der Betroffenen zur Datenverarbeitung von personenbezogenen Daten ist vor Gesetz dann gegeben, wenn sie frei, ohne Zwang, in Kenntnis der Sachlage und fallbezogen abgegeben wurde.

# Notizen

# Notizen

# Werden Sie Mitglied...

## ...weil wir gemeinsam mehr erreichen können.

Die Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier (GPA-djp) verhandelt **jährlich mehr als 150 Kollektivverträge** und sichert damit das Einkommen der unselbstständig Beschäftigten.

## **Jetzt** Mitglied werden!

❑ Frau ❑ Herr Akad. Grad .....

Familienname .....

Vorname .....

SV-Nr./Geburtsdatum | | | | | | | | | | |

Straße/Hausnr. .....

PLZ/Wohnort .....

Telefon .....

E-Mail .....

❑ Angestellte/r ❑ Arbeiter/in ❑ SchülerIn
❑ geringfügig beschäftigt ❑ freier Dienstvertrag ❑ StudentIn
❑ dzt. ohne Beschäftigung ❑ Lehrling ❑ Werkvertrag

Derzeitige Tätigkeit .....

Damit wir Sie bei Kollektivvertragsverhandlungen richtig informieren können, bitten wir um Angabe Ihres Dienstgebers und der genauen Branche. Ihre Angaben werden **streng vertraulich** behandelt.

Beschäftigt bei **Firma** (bzw. Schule/Universität) .....

Anschrift .....

**Branche** (z. B. Elektroindustrie, Spedition, Baugewerbe, Bank, Versicherung, Innen- oder Außendienst, Verein, Lebensmittelhandel bzw. Schul-/Studienrichtung)

.....

Die Beitragszahlung erfolgt mit **Einzugsermächtigungsverfahren**.
Hiermit ermächtige ich Sie **widerruflich**, die von mir zu entrichtenden Zahlungen bei Fälligkeit zu Lasten meines Kontos mittels Lastschrift einzuziehen. Damit ist auch meine kontoführende Bank ermächtigt, die Lastschriften einzulösen, wobei für diese keine Verpflichtung zur Einlösung besteht, insbesondere dann, wenn mein Konto die erforderliche Deckung nicht aufweist. Ich habe das Recht, innerhalb von 56 Kalendertagen ab Abbuchungstag ohne Angabe von Gründen die Rückbuchung bei meiner Bank zu veranlassen. Ich ermächtige die Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier (GPA-djp) den folgenden Mitgliedsbeitrag (= 1 % meines Bruttogehaltes/Bruttolohnes, meiner Bruttolehrlingsentschädigung bzw. Grenzbeitrag) von meinem unten angeführten Konto einzuziehen.

Höhe des monatlichen Beitrages: **EUR** | | | | | |

❒ monatlich ❒ alle 2 Monate ❒ jedes Quartal ❒ 1/2 jährlich
❒ jährlich (Schüler-/StudentInnen)

Konto-Nr. | | | | | | | | | | |

Geldinstitut .....Bankleitzahl.....

Monat/Jahr der erstmaligen Einzahlung .....

GPA-djp-Beitrittsmonat/-jahr .....

**Datum/Unterschrift**.....
(Diese Unterschrift gilt gleichzeitig als Berechtigung für o.a. Einzugsermächtigungsverfahren.)

1034 Wien, Alfred-Dallinger-Platz 1, Tel 05 0301-301, Fax 05 0301-300, E-Mail: service@gpa-djp.at, **www.gpa-djp.at**

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Bitte hier abtrennen.

**AbsenderIn:**

Bitte ausreichend frankieren

**GEWERKSCHAFT**
**DER PRIVATANGESTELLTEN, DRUCK,**
**JOURNALISMUS, PAPIER**
Alfred-Dallinger-Platz 1
1034 Wien

# Adressen

**GPA-DJP Zentrale**
1034 Wien, Alfred-Dallinger-Platz 1
Telefon: 05 0301-301, Fax: 05 0301-300
**Interessengemeinschaften**
Telefon: 05 0301-21314, Fax: 05 0301-71314
**Grundlagenabteilung/Arbeit und Technik**
Telefon: 05 0301-21218, Fax: 05 0301-71218

**GPA-DJP Regionalgeschäftsstelle Wien**
1034 Wien, Alfred-Dallinger-Platz1
Telefon: 05 0301-21000
E-Mail: wien@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Niederösterreich**
3100 St. Pölten, Gewerkschaftsplatz 1
Telefon: 05 0301-22000
E-Mail: niederoesterreich@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Burgenland**
7000 Eisenstadt, Wiener Straße 7
Telefon: 05 0301-23000
E-Mail: burgenland@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Steiermark**
8020 Graz, Karl-Morre-Straße 32
Telefon: 05 0301-24000
E-Mail: steiermark@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Kärnten**
9020 Klagenfurt, Bahnhofstr. 44/4
Telefon: 05 0301-25000
E-Mail: kaernten@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Oberösterreich**
4020 Linz, Volksgartenstrasse 40
Telefon: 05 0301-26000
E-Mail: oberoesterreich@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Salzburg**
5020 Salzburg, Markus-Sittikus-Str. 10
Telefon: 05 0301-27000
E-Mail: salzburg@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Tirol**
6020 Innsbruck, Südtiroler Platz 14-16
Telefon: 05 0301-28000
E-Mail: tirol@gpa-djp.at

**GPA-DJP Regionalgeschäftsstelle Vorarlberg**
6900 Bregenz, Reutegasse 11
Telefon: 05 0301-29000
E-Mail: vorarlberg@gpa-djp.at


**www.gpa-djp.at**

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

1034 Wien, Alfred-Dallinger-Platz 1 - Telefon 05 0301-301 - www.gpa-djp.at - E-Mail: gpa@gpa-djp.at
DVR 0046655 - ZVR 576439352