

Einführung zum Datenschutz

Datenschutz - Erfordernis

- Datenschutz bedeutet:
 - „Schutz der Persönlichkeitsrechte“
- Persönlichkeitsrechte ist konkretisiert durch Rechtsprechung und herrschende Meinung
 - Recht am eigenen Bild
 - Recht am eigenen Wort
 - Recht am Charakterbild
 - Recht der Ehre
 - Recht auf Achtung der Privatsphäre
 - Recht auf informationelle Selbstbestimmung

Datenschutz - Erfordernis

- Recht am eigenen Bild
 - Schutz vor jeder Art unbefugter Verbreitung und Veröffentlichung
 - Schutz vor unbefugter Anfertigung

- Recht am eigenen Wort
 - Selbstbestimmung, wem das gesprochene Wort gilt und wie es weiter verwendet werden darf
 - Verbot der akustischen Überwachung durch technische Geräte
 - Unzulässigkeit des Abhörens/Mithörens ohne Einwilligung

Datenschutz - Erfordernis

- Recht am Charakterbild
 - Schutz vor unbefugter Ausforschung der Strukturen und Eigenschaften einer Person
- Recht an der Ehre
 - Schutz vor Beleidigung, übler Nachrede oder sonstiger sozialen Diffamierung

Datenschutz - Erfordernis

- Recht auf Achtung der Privatsphäre
 - Inhalt und Umfang des Fragerechts
 - Ärztliche Untersuchung
 - Leibesvisitation und Torkontrollen
 - Aushang von Abmahnungen und ähnlichem

- Recht auf informationelle Selbstbestimmung
 - „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“
 - Einschränkung bedarf gesetzlicher Regelungen

Informationelles Selbstbestimmungsrecht

”Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. ”

Auszug Bundesverfassungsgericht-Urteil vom 15.12.1983

Recht in Deutschland und Europa

- Normative Vorgaben des Bundesdatenschutzgesetzes (BDSG)
 - zur Auftragsdatenverarbeitung
 - zur grenzüberschreitenden Datenverarbeitung
- Normative Vorgaben der EG-Datenschutzrichtlinie
- Spezifische EU-Regelungen zur Auftragsdatenverarbeitung

Datenverarbeitung im Auftrag

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

- (1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.
- (2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
- (3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
- (4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für
 - a) öffentliche Stellen,
 - b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,
- die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.
- (5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Datenverarbeitung im Auftrag

Vorgaben durch § 11 BDSG:

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

Datenverarbeitung im Auftrag

Vorgaben durch § 11 BDSG:

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

Datenverarbeitung im Auftrag

Arten von Auftragsdatenverarbeitung:

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

Datenübermittlung ins Ausland

§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

- (1) Für die Übermittlung personenbezogener Daten an Stellen
 - in anderen Mitgliedstaaten der Europäischen Union,
 - in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder der Organe und Einrichtungen der Europäischen Gemeinschaftengelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.
- (2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.
- (3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Landesregeln und Sicherheitsmaßnahmen herangezogen werden.
- (4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.
- (5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.
- (6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden

§ 4b BDSG: Übermittlung personenbezogener Daten ins Ausland

- Innerhalb der Mitgliedstaaten der EU sieht das BDSG „freien Datenverkehr“ vor (§§ 28 – 30 BDSG)
- Folge ist, dass die Bewertung des Datenverkehrs von Leipzig nach Berlin identisch zu werten ist wie der von Leipzig nach Paris
- Datentransfer in Drittländer, die sich außerhalb der EU befinden, ist nur dann zulässig, wenn das Drittland ein angemessenes Datenschutzniveau gewährleistet

§ 4b BDSG: Übermittlung personenbezogener Daten ins Ausland

- Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung der Umstände beurteilt
- Die Verantwortung für die Übermittlung trägt die übermittelnde Stelle
- Der Empfänger ist darauf hinzuweisen, dass Daten ausschließlich nach deren Zweck zu verarbeiten sind

§ 4c BDSG: Ausnahmen

Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern ...

§ 4c Ausnahmen

- (1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern
 - der Betroffene seine Einwilligung gegeben hat,
 - die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
 - die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
 - die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
 - die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
 - die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.
 - Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.
- (2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei den Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.
- (3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

Zweckbindung gemäß § 4c

- Die Stelle, die Daten erhält, ist auf die enge Zweckbindung hinzuweisen
- Ihr wachsen im Regelfall keine eigenständigen Verarbeitungskompetenzen zu
- Ergebnis der Verarbeitung ist somit das Resultat der zuvor festzulegenden Zweckbindung

Anwendungsbereich

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

Angemessenes Datenschutzniveau

- Ursprünglich sollte es *Gleichwertigkeit* heißen
- Ist nicht ein Vergleich nationaler gesetzlicher Voraussetzungen
- Nach § 4b werden insbesondere herangezogen:
 - Art der Daten
 - Zweckbestimmung
 - Dauer der geplanten Verarbeitung
 - Herkunfts- und Empfängerland
 - für den Empfänger geltende Rechtsnormen und Sicherheitsmaßnahmen
- Die Verantwortung für die Übermittlung trägt die übermittelnde Stelle in Person des bDSB

Vorgaben der EU-DSR

- Bildet Grundlage für den freien Datenverkehr innerhalb der EU
- Mindeststandard des gesetzlichen Datenschutzes in allen von der Richtlinie erfassten EU-Staaten
- Bewertung des Schutzniveaus in Drittländern (Art. 30 DSR) durch die EU-Datenschutzgruppe („Art. 29-Gruppe“)

EU/EWR-Staaten

- In der EU ist der Datenverkehr, wie zuvor festgestellt, „frei“
- Zu den EWR-Staaten gehören derzeit:
 - Norwegen
 - Island
 - Lichtenstein

Drittländer

- Generell alle Nationen außerhalb der EU bzw. des EWR
- Drittländer, bei denen die EU-Kommission ein angemessenes Niveau festgestellt hat, sind:
 - Argentinien
 - Guernsey
 - Schweiz
 - Ungarn
 - Kanada (begrenzt)
 - USA (stark begrenzt))
- Für alle anderen Nationen gilt, dass vor Datentransfer ein gesonderter, umfangreicher Vertrag über das zu errichtende Datenschutzniveau nach europäischem Vorbild abzuschließen ist

Safe Harbor Principles

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

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

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

Standardvertragsklauseln der EU

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

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

Inhalt der EU-Klausel

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

Code of Conduct

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

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

Hierbei sind zumindest die Regelungen des BDSG einzuhalten.

Aber ...

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

Zulässigkeitskriterien

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

Umgang mit Arbeitnehmerdaten - Beispiele -

Die Beispiele

National

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

International

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

1. Zentralisierung von Aufgaben im deutschen Konzern

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

2. Auslagerung von Verwaltungsaufgaben an ein externes Unternehmen

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

3. Weltweiter Datenaustausch innerhalb eines Konzerns

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

4. Leistungskontrolle in einem Drittland

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

5. Buchhaltung in Indien

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

6. Vertrieb in Prag vs. Goa

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

7. Skill-Management in der Karibik

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

Noch Fragen ???



DAS WAR`S

Vielen

Dank

Für Eure

Aufmerksamkeit!

Sie sind hier: [▶ Home](#)

Willkommen bei der TBS Niedersachsen!

Wir sind eine gemeinnützige Beratungseinrichtung mit dem Auftrag, die technologische, soziale und ökologische Modernisierung in niedersächsischen Betrieben und Verwaltungen zu fördern und zu begleiten.



AuG	OE	PE	AO	DS	IT
Arbeits- und Gesundheits- schutz	Organisations- entwicklung	Personal- entwicklung	Arbeits- organisation	Datenschutz	Informations- technik

**Aktuelle
Veranstaltungen**

- "Fachtagung Arbeits- und Gesundheitsschutz"
05. Oktober 2006
[▶ Mehr Infos](#)
- "Zielvereinbarungen und Entgelt"
09. - 11. Oktober 2006
[▶ Mehr Infos](#)
- "Bilanzen, Kennzahlen, Jahresabschluss"
10. - 12. Oktober 2006
[▶ Mehr Infos](#)

News [▶ Alle News](#)

- TBS-FACHTAGUNGEN:
Datenschutz-
Fachtagung 2006
[▶ Mehr Infos](#)
- Arbeits- und
Gesundheitsschutz
Fachtagung 2006
[▶ Mehr Infos](#)