1. Datenschutzrechtliche Grundlagen

Beim Bundesdatenschutzgesetz (BDSG) handelt es sich um ein „Verbotsgesetz mit Erlaubnisvorbehalt“, d.h. das **Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist grundsätzlich verboten**, es sei denn, dass der **Betroffene eingewilligt** hat oder entsprechende **Erlaubnistatbestände** ausdrücklich vorliegen (§ 3 (1) BDSG).

Das BDSG richtet sich an die **„verantwortliche Stelle“**, d.h. Person oder Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 (7) BDSG).

Erlaubnistatbestände sind in den gesetzlichen Ausnahmekatalogen des BDSG zu finden, in anderen Gesetzen (z.B. Teledienstedatenschutzgesetz (TDDSG), Telekommunikations-Datenschutzverordnung (TSDV)).

Das Datenschutzrecht schützt **„personenbezogene Daten“** (§ 4 (1) BDSG). Dabei handelt es sich um Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (auch Betroffener genannt). Darüber hinaus kennt das Gesetz auch noch die Subkategorie der **„besonderen Arten personenbezogener Daten“** („sensitive Daten“). Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit...

2. Datenschutz im Arbeitsverhältnis

Datenschutz und Arbeitsrecht treffen in der Praxis häufig aufeinander, besonders in den folgenden drei Themenkreisen:

2.1. Einsatz von Personalverwaltungssystemen

Unternehmen setzen Datenbanken und Verwaltungssystemen zur Personalverwaltung und Gehaltsabrechnung und häufig auch für so genannte „Skills-Datenbanken“ ein, um Fähigkeiten und Qualifikationen der Arbeitnehmer zu speichern. Unternehmen verfolgen damit das Ziel, für bestimmte Aufgaben eine schnelle, gezielte Auswahl geeigneter Arbeitnehmer mit entsprechenden Fähigkeiten treffen zu können. Der Einsatz der Technologien beruht dabei aus datenschutzrechtlicher Sicht auf einem der nachfolgenden Erlaubnistatbestände:

Erlaubnistatbestand nach § 28 (1) S.1 Nr. 1

Nach § 28 (1) S.1 Nr. 1 ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten in dem Umfang zulässig, soweit sie der Zweckbestimmung eines Vertragsverhältnisses dient. Folglich sind sämtliche Datenverarbeitungsvorgänge ohne Einwilligung des jeweils Betroffenen möglich. Dieser Grundsatz gilt auch für „sensitive Daten“. Daher dürfen auch insbesondere die Religionszugehörigkeit (zur Berechnung der Kirchensteuer) sowie die krankheitsbedingten Fehlzeiten (zur Entgeltfortzahlung) erfasst werden.

Erlaubnisatbestand nach § 28 (1) S.1 Nr. 2

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist zulässig, soweit dies zur Wahrung berechtigter Interessen der „verantwortlichen Stelle“ (hier: Arbeitgeber) erforderlich ist. Es dürfen jedoch keine schutzwürdigen Interessen des Betroffenen (Arbeitnehmer) verletzt werden.

Wie wird **„berechtigtes Interesse“** definiert? – Der Begriff wird weitgefasst und umfasst jedes von der Rechtssprechung gebilligtes Interesse, einschließlich wirtschaftlicher und ideeller Interessen. Eine Erhebung, Verarbeitung und Nutzung zur Wahrung dieser Interessen ist jedoch nur dann zulässig, wenn es für den Arbeitgeber keine wirtschaftlich zumutbaren Alternativen gibt, die die Verwendung der Daten erübrigen würde. (Beispiel siehe Folien).

Erlaubnistatbestand: Einwilligung des Arbeitnehmers

Sofern die Datenverarbeitung weder über § 28 (1) Nr. 1 BDSG oder § 28 (1) Nr. 2 BDSG noch einen anderen gesetzlichen Ausnahmetatbestand gerechtfertigt werden kann, muss die Einwilligung des Arbeitnehmers eingeholt werden. (§ 4 BDSG).

Die Einwilligung muss ausdrücklich und schriftlich erklärt werden (§ 4a (1) S. 3 BDSG). Dies erfordert, dass der Betroffene vor der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten detailliert informiert wird über die Identität der verantwortlichen Stelle, die betroffene Datenkategorie, den Zweck der Datenerhebung, -verarbeitung und –nutzung, zugriffsberechtigte Personen, mögliche Empfänger der Daten, weitere Informationen, die für die Entscheidungsfindung des Betroffenen relevant sein können.

Dem Arbeitgeber steht ein eingeschränktes Informationsrecht zu, d.h. es sind noch solche **Fragen zulässig**, die **in direktem Zusammenhang mit der zu übernehmenden Aufgabe des Arbeitsnehmers stehen** und auch hierfür nur von Bedeutung sind.

Erlaubt sind demzufolge Fragen nach…

… Qualifikation

… beruflicher Werdegang

Verboten hingegen sind Fragen nach…

… Schwangerschaft

… späterem Kinderwunsch

… Vorstrafen

… laufenden Strafverfahren

… Krankheiten

… Körperbehinderung

Erlaubnistatbestand: Betriebsvereinbarungen

Nach Literatur und herrschender Meinung stellen auch Betriebsvereinbarungen eine Erlaubnisnorm im Sinne des BDSG dar.

2.2. Übermittlung von personenbezogenen Daten im internationalen Konzern

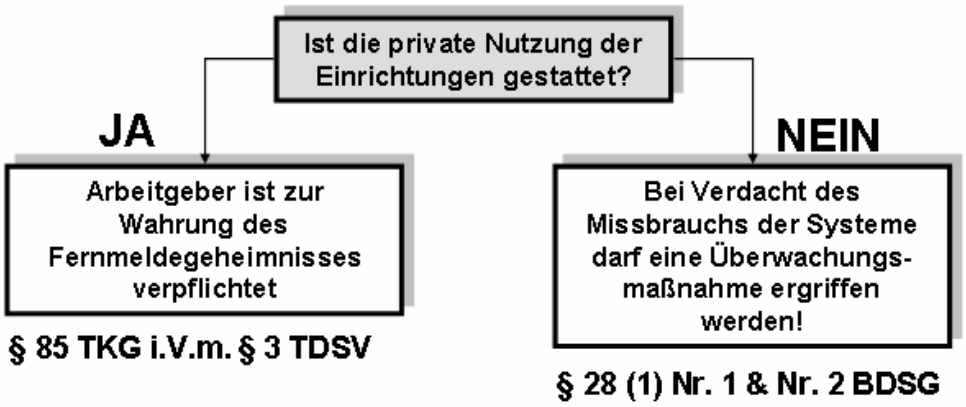
- **„Übermittlung innerhalb der EU und EWR“:** Übermittlung innerhalb den Mitgliedsstaaten von EU (Europäische Union) und EWR („Europäischer Wirtschaftsraum“), solange auch die Übermittlung innerhalb von Deutschland zulässig ist.
- **„Übermittlung in Länder außerhalb von EU und EWR“**: Übermittlung von personenbezogenen Daten in Drittländer (also außerhalb der Mitgliedstaaten), hat zu unterbleiben, wenn der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, besonders wenn beim Empfänger ein angemessenes Schutzniveau nicht gewährleisten kann.

  Eine Übermittlung von personenbezogenen Daten in Drittländer ist nur dann nicht verboten, wenn eine der folgenden Garantien für ein angemessenes Datenschutzniveau vorliegen:

  - **Vertragsklauseln:** Die EU-Kommission stellt Standardvertragsklauseln zur Verfügung, d.h. verbindliche Klauseln für die Datenübermittlung zwischen zwei verantwortlichen Stellen.
  - **Unternehmensrichtlinien:** Große Konzerne haben eigene, unternehmensinterne „Richtlinien“
  - **Safe-Harbor-Regeln:** Unternehmen in den USA müssen, sich nach den Safe-Harbor-Regeln zertifizieren lassen, indem sie bestimmte interne Verfahren und Praktiken einführen (siehe Safe-Harbor Liste im Internet)

2.3. Email- und Internetüberwachung durch den Arbeitgeber

Darf ein Arbeitgeber seine Arbeitnehmer bei der Nutzung von Kommunikationseinrichtungen (Telefon, Email und Internet) kontrollieren?



3. Datenschutz bei Internetverträgen

3.1 Anwendbares Recht

TDDSG (Teledienstedatenschutzgesetz) & **BDSG** (Bundesdatenschutzgesetz)

Territorialprinzip:
Das deutsche Datenschutzrecht findet auf Sachverhalte Anwendung, wenn Daten in Deutschland erhoben, verarbeitet oder genutzt werden.

(Wiki: Generell sagt das Territorialitätsprinzip, dass alle Personen der Oberhoheit und den Gesetzen des Staates unterworfen sind, auf dessen Territorium sie sich jeweils befinden.)

Zwei Ausnahmen:

- ⇒ Es gilt statt des Territorialprinzips das Sitzlandprinzip, wenn die verantwortliche Stelle, welche die Daten erhebt, verarbeitet oder nutzt innerhalb der EU sitzt **und** der Umfang der Tätigkeit in Deutschland so beschränkt ist, dass hierdurch keine Niederlassung der verantwortlichen Stelle in Deutschland begründet wird.
- ⇒ Das deutsche Datenschutzrecht gilt entgegen dem Territorialprinzip, wenn die Verantwortliche Stelle nicht in Deutschland sondern außerhalb der EU und des EWR (Europ. Wirtschaftsraum) sitzt und auf automatisierte oder nicht automatisierte Mittel zugreift, die in Deutschland belegen sind.

Für den im außereuropäischen Ausland sitzenden Datenverarbeiter ohne Niederlassung in Deutschland gilt trotz des Territorialprinzips deutsches Datenschutzrecht, wenn er auf automatisierte oder nicht automatisierte Mittel in Deutschland auf die Daten zugreift und diese kontrolliert.

3.2 Gesetzliche Regeln

TDDSG & BDSG sind **Verbotsgesetzte** mit Erlaubnisvorbehalten.

- **Bestandsdaten(§5TDDSG):**
  Zu den Bestandsdaten zählen insbesondere Personalien des Nutzers und Informationen über den Abrechnungsmodus, soweit diese Daten für den betreffenden Teledienst unerlässlich sind. -> Daher fallen bei kostenlos angebotenen Dienstens in der Regel keine Bestandsdaten an.

- **Nutzungsdaten (§6 I TDDSG):**
  Nutzungsdaten sind die Daten, die während der Nutzung eines Teledienstes entstehen (z.B. Systemdaten, Nutzererkennungen und Passwörter), aber auch die Daten die bei interaktiven Spielen oder elektronischen Zeitschriften anfallen.

- **Abrechnungsdaten (§6 I, IV TDDSG)**
  Abrechnungsdaten sind eine Unterkategorie der Nutzungsdaten und bezeichnen diejenigen Daten, die für Abrechnungszwecke erforderlich sind. Sie dürfen über das Ende des eigentlichen Nutzungsvorgangs hinaus verarbeitet und genutzt werden, sofern sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind oder wenn sie für die Aufklärung von missbräuchlicher Inanspruchnahme des Dienstes verwendet werden sollen (§6 VIII TDDSG)

Für Daten, die den Inhalt der Kommunikation betreffen, findet das BDSG Anwendung. Im Wesentlichen §28 BDSG.
Man muss streng danach abgrenzen, ob die gesamte Leistung mittels Teledienstes erbracht wird (TDDSG) oder nicht (BDSG)!

Cookies, Nutzerprofile
Der Nutzer muss über den Einsatz von Cookies ausdrücklich informiert werden.(§4 TDDSG)
Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. (§6 III TDDSG)

3.3 Website Privacy Policies

Nach deutschem Recht sind sie überflüssig. Da sie den Nutzer nicht lediglich informieren, sondern versuchen darüber hinaus Rechte und Pflichten zu begründen -> kann dies zum Nachteil für Websitenbetreiber führen.

Das Anbieten von kostenlosen Informationen über das Internet stellt grundsätzlich keine Vertragsbeziehung zwischen Anbieter und Nutzer her.
ABER: Vertragsverhältnis kann mit Hilfe von Datenschutzerklärungen geschaffen werden.

TDG, TDDSG und BDSG verpflichten den Anbieter den Nutzer über die Datenverarbeitung zu informieren und ihn über seine diesbezüglichen Rechte zu belehren.Eine Aussage, dass die Gesetze eingehalten werden genügt nicht. Die Klauseln müssen transparent, leicht verständlich, wahr, richtig und vollständig sein. Der Nutzer darf nicht getäuscht werden.
Unvollständig sowie pauschal gehaltene Beschreibungen von Datenverarbeitungsvorgängen sind unzulässig.