Datenschutz ist Chefsache!

Ralf Essl
Geprüfter Datenschutzbeauftragter (FH)
Beratung CAD/CAM/PDM

RE Engineering und Consulting
Hochalmstraße 5
81825 München

Datenschutz
Zur Einstimmung

Die letzte Stimme, die man hört, bevor die Welt explodiert, wird die Stimme eines Experten sein, der sagt: „Das ist technisch unmöglich!“

(Sir Peter Ustinov, engl. Schauspieler und Schriftsteller)

Was passieren kann, wird…

(Murphy´s Law)

It´s no bug, it´s a feature!

(Bill Gates bei einer Präsentation eines neuen Betriebssystems)

Datenschutz
Ziele von Unternehmen

- Zugang zu globalen Märkten

- Die Unternehmen betreten neue geografische Märkte mit fremden Kulturen, unbekannten Umfeldbedingungen und Rechtspositionen.

- Die ökonomischen, politischen und rechtlichen Rahmenbedingungen für unternehmerisches Handeln ändern sich rasant und steigern Chancen und Risiken des Geschäfts.

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Datenschutz
Gesetzliche Bestimmungen KonTraG

KonTraG: „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG) vom 1. Mai 1998

§ 91: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

Von den Bestimmungen des KonTraG sind auch die Gesellschaften betroffen, die zwei der drei nachfolgenden Kriterien erfüllen:

- ✓ Bilanzsumme > 3,44 Mio. EUR
- ✓ Umsatz > 6,87 Mio. EUR
- ✓ Mitarbeiterzahl > 50

Datenschutz
Verantwortliche <=> Konsequenzen

Verantwortliche

- ✓ Vorstände von Aktiengesellschaften
- ✓ Aufsichtsräte
- ✓ Geschäftsführer von GmbH
- ✓ IT-Leiter
- ✓ Prüfungsgesellschaft

Konsequenzen

- ✓ Geldbußen
- ✓ Schadenersatz gegen Gesellschaft
- ✓ Schadenersatz gegen Geschäftsführer/Vorstand
- ✓ Rechenschaft für IT-Verantwortliche

Datenschutz
Was ist in einem Unternehmen zu tun?

- ⇨ Systematische und kontinuierliche Erfassung der Risiken
- ⇨ Analyse und Beurteilung der Risiken
- ⇨ Erkennen der Kumulation von Einzelrisiken zur Bestandsgefährdung
- ⇨ Schaffung von Regeln für den Umgang mit Einzelrisiken
  Kommunikation der Risiken
- ⇨ Frühzeitiges Ergreifen geeigneter Maßnahmen
- ⇨ Überprüfung der Funktionsfähigkeit der Maßnahmen durch umfassende Prüfung

Ziel: Schutz der Werte (auch Daten) des Unternehmens

Datenschutz
Motivation für Unternehmen

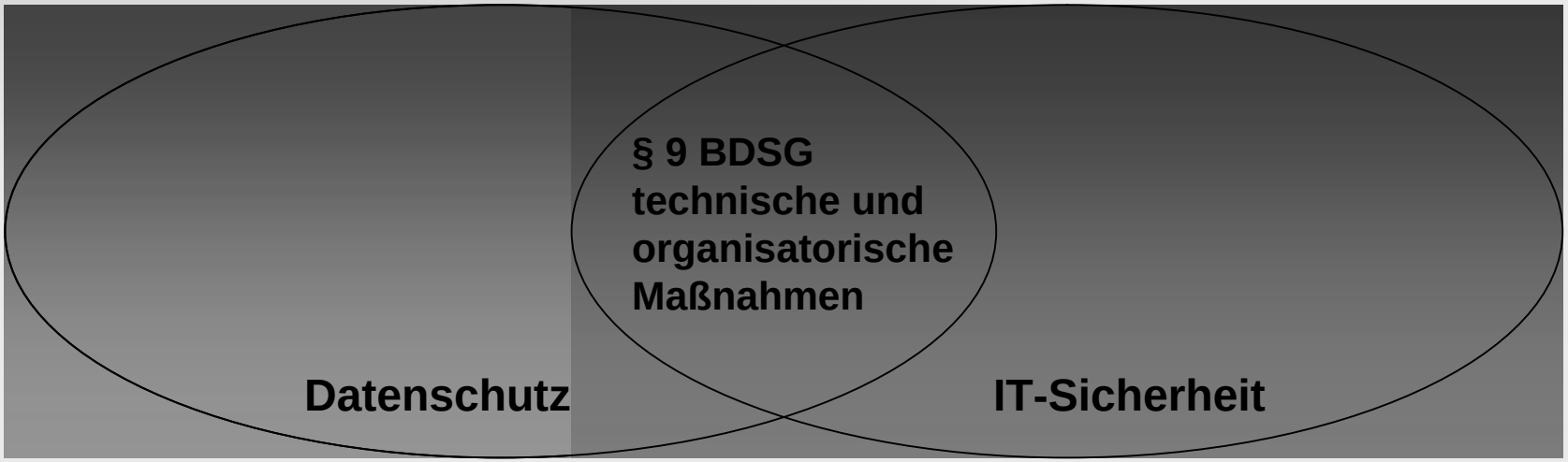
Die Motivationen für Unternehmen sich mit Informationssicherheit auseinander zu setzen sind vielfältig

...und lassen sich in einem Drei Säulen Modell darstellen.

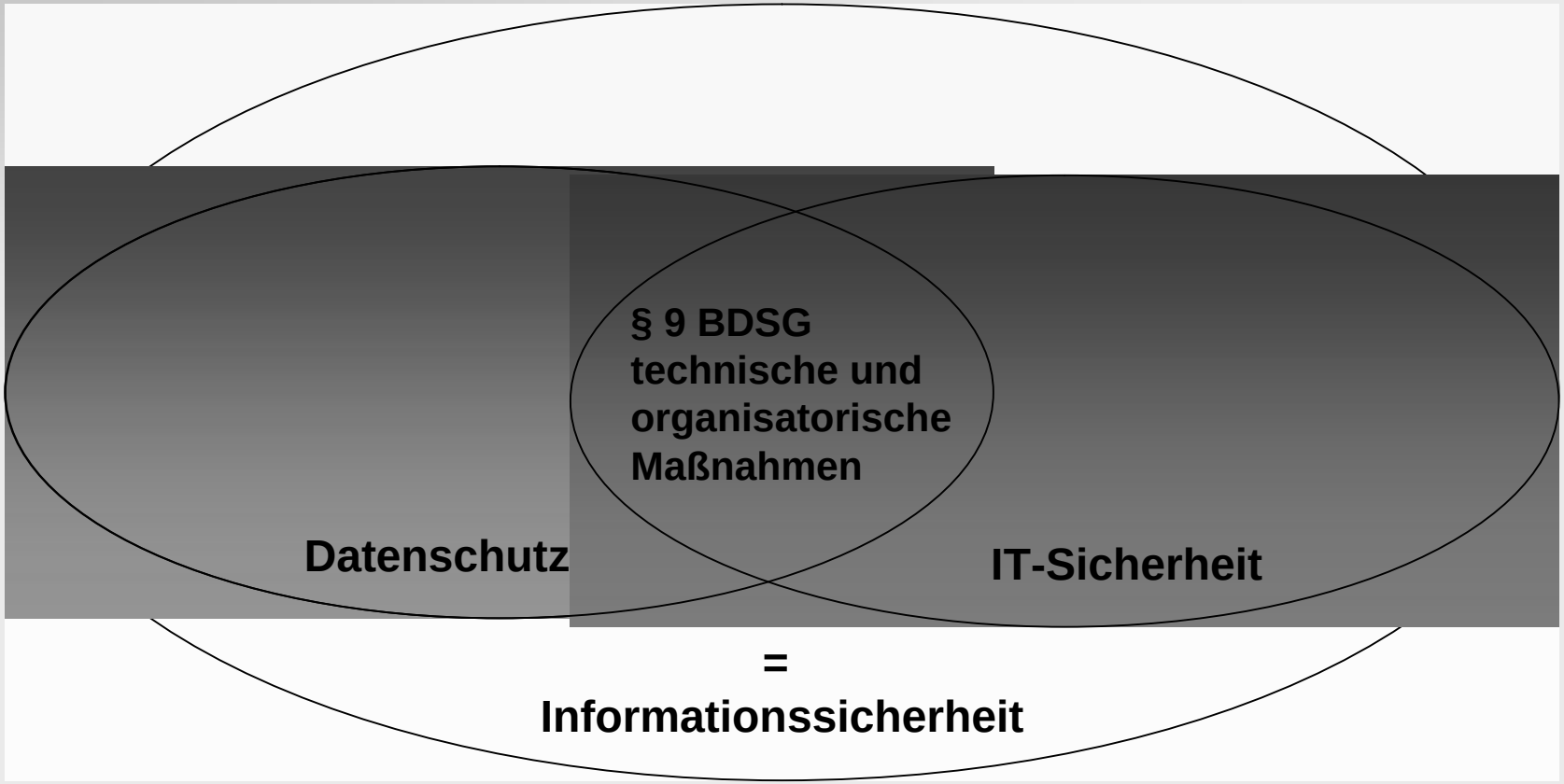
Eigeninteresse	Rechtliche Vorgaben	Stakeholder
▪ Schutz von Informationen und Wissen ▪ Schutz der Investitionen ▪ Schutz der Infrastrukturen ▪ Image in der Öffentlichkeit	▪ Risikoabsicherung Versicherungen, Eigenkapital **(Basel II)** ▪ Gesetz zur Kontrolle und Transparenz in Unternehmens-bereichen **(AktG/KonTraG)** ▪ Datenschutz **(Teledienstedatenschutz, Informations- und Kommunikations-dienstegesetz, BDSG)** ▪ Allgemeine Geheimhaltungspflichten / Bankgeheimnis (**KWG**) ▪ Auskunft- und Nachweispflichten **(GoBF/BMF, HGB, Steuerrecht, ...)**	▪ Kunden fordern zuverlässige und **verfügbare Service-Leistungen** ▪ Kunden fordern **Schutz der persönlichen Daten** ▪ Investoren fordern **Corporate Governance**

Datenschutz

Datenschutz <=> Datensicherheit



Datenschutz und IT-Sicherheit = Informationssicherheit



Datenschutz
Was ist das?

„Der Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“
(BDSG § 1 Absatz 1)

Datenschutz
Was sind personenbezogene Daten?

„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“
(BDSG § 3 Absatz 1)

Datenschutz
Beispiele personenbezogener Daten

Beispiele personenbezogener Daten:

- ✓ Geschlecht
- ✓ Titel
- ✓ akademische Grade
- ✓ Vorname
- ✓ Name
- ✓ Anschrift
- ✓ Geburtsdatum
- ✓ Telefonnummer
- ✓ Telefaxnummer
- ✓ E-Mail Adresse
- ✓ IP-Nummer
- ✓ arbeitsrechtliche Rechtsverhältnisse
- ✓ Steuerklasse
- ✓ Kontonummer
- ✓ Versicherungsnummer
- ✓ KFZ-Kennzeichen
- ✓ Krankheiten
- ✓ Ordnungswidrigkeiten
- ✓ strafbare Handlungen
- ✓ usw.

Datenschutz
Beispiele diverser Anforderungen

Beispiele diverser Anforderungen an ein Unternehmen:

- ⇨ ERP-Systeme
- ⇨ Groupwaresysteme wie Exchange, Lotus, GroupWise
- ⇨ Telefonanlagen
- ⇨ CTI/UMS Systeme
- ⇨ Gesprächsdatenverarbeitung
- ⇨ E-Mail mit Anti-Spam-Programmen
- ⇨ Arbeitszeiterfassung
- ⇨ Niederlassungen, Mitarbeiter, Kunden, Lieferanten im In- und Ausland
- ⇨ usw.

Datenschutz
Externe Auftragsdatenverarbeitung

Bei externer Auftragsdatenverarbeitung sind mit der beauftragten Stelle rechtsverbindliche Vereinbarungen bezüglich des Datenschutzes zu vereinbaren.

- Die externe Stelle ist regelmäßig auf die Einhaltung des Datenschutzes nach BDSG zu kontrollieren.

Datenschutz
Was ist das „Jedermannsrecht“ ?

- Jede Person kann auf Wunsch Einsicht in die Verfahrensbeschreibung nach § 4e BDSG verlangen
- Angaben (ohne technische/organisatorische Maßnahmen und ohne Zugriffsberechtigungen) in geeigneter Weise müssen „Jedermann“ zeitnah zur Verfügung gestellt werden.

„Jedermann“ kann die Aufsichtsbehörde anrufen.

Dies wird häufig aus Gründen des Wettbewerbs aus Konkurrenzgründen getätigt.

Datenschutz
Heute im Unternehmen?

- BDSG und mehr als 500 (!) weitere Vorschriften (Anzahl stetig steigend)
- Hohe Änderungsquote der Vorschriften
- Viele zum Teil widersprüchliche Urteile
- Komplexe IT-Landschaft

Hohe Anforderungen an den Datenschutzbeauftragten

Datenschutz
Pflicht zur Bestellung?

BDSG § 4f

Sind mehr als **vier** Personen mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt, ist ein Datenschutzbeauftragter zu bestellen.

Keine Wahlfreiheit, sondern Pflicht

Datenschutz
Bußgelder bis hin zur Freiheitsstrafe!

Zur Durchsetzung des Datenschutzes stehen der Aufsichtsbehörde folgende Sanktionsmöglichkeiten zur Verfügung:

- ⇨ Bußgelder bis 25.000,00 € bei Verstößen gegen formale Vorschriften
- ⇨ Bußgelder bis 250.000,00 € gegen inhaltliche Vorschriften
- ⇨ Strafanzeigen (bisher nur direkt durch den Betroffenen)

Einhaltung der Gesetze oder Risikobereit?

Datenschutz
Reaktion der Aufsichtsbehörden

- Auffassung vieler Aufsichtsbehörden:

  „Ein Unternehmen soll nicht dafür bestraft werden, dass es sich mit dem Datenschutz beschäftigt und seine Fragestellung hierzu an die Aufsichtsbehörde heranträgt.“

- Auch oder gerade für den Datenschutz gilt daher:

Prävention ist besser als Sanktion

Datenschutz
Praktische Arbeit des DSB

Tätigkeiten des DSB, die für die Aufsichtsbehörde wichtig sind:

- ⇨ Ein kompetenter Ansprechpartner in allen Fragen des Datenschutzes im Unternehmen für die Aufsichtsbehörde
- ⇨ Führen der Verfahrensverzeichnisse nach § 4g Abs. 2 BDSG
- ⇨ Umsetzen der evtl. Meldepflicht nach § 4e BDSG
- ⇨ Sicherstellen der Verpflichtung auf das Datengeheimnis nach § 5 BDSG
- ⇨ Schulung der Mitarbeiter/innen in Datenschutzfragen
- ⇨ Sensibilisierung des Managements für den Datenschutz

Datenschutz
Mitwirkung des DSB bei Kontrollen

Die zu kontrollierende Stelle sowie die Leitungen dieser Stellen haben der Aufsichtsbehörde alle für Ihre Arbeit erforderlichen Auskünfte unverzüglich zu erteilen:

- ⇨ Der DSB sollte die Antworten auf mögliche Auskunftsverlangen oder zumindest den zuständigen Ansprechpartner kennen
- ⇨ Dadurch kann die Prüfung für beide Seiten effizient gestaltet werden
- ⇨ Ein kompetenter DSB kann Augenmerk auf umgesetzte Maßnahmen und sonstige positiven Aspekte im Bezug auf den Datenschutz lenken

Bestellung zum Datenschutzbeauftragten

§ 4 Abs. 2 BDSG

⇨ Zum Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche

- **Fachkunde und**
- **Zuverlässigkeit besitzt**.

⇨ Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden.

Kompetenzen des Datenschutzbeauftragten

Fachkompetenz
- Rechtskenntnisse
- IT-Kenntnisse
- Betriebsorganisationskenntnisse

Methodenkompetenz
- Erstellung von Datenschutzkonzepten
- Durchführung von Datenschutzaudits
- Didaktische Fähigkeit

Unternehmerische Kompetenz
- Wirtschaftliches Denken
- Visionäres Denken
- Planungsfähigkeit

Führungskompetenz
- Überzeugungskraft
- Motivationsfähigkeit
- Organisationstalent
- Kontrollfähigkeit

Sozialkompetenz
- Problem- und Konfliktlösungsfähigkeit
- Teamfähigkeit
- Verschwiegenheit
- Zuverlässigkeit

Aufgaben im Datenschutzmanagement

Auszug - Teil 1

- ⇨ Analyse aller Prozesse auf Verarbeitung von personenbezogenen Daten
- ⇨ Datenschutz-Schwachstellen
- ⇨ Beratung der Unternehmensleitung hinsichtlich Datenschutzmaßnahmen und deren Umsetzung
- ⇨ Erstellung einer internen Datenschutzrichtlinie
- ⇨ Erarbeitung und Realisierung eines Datenschutzkonzeptes
- ⇨ Erstellung eines IT-Sicherheitskonzeptes
- ⇨ Schulungskonzept und Schulungen für die Mitarbeiter
- ⇨ Erstellen von Betriebsanweisungen

Aufgaben im Datenschutzmanagement

Auszug - Teil 2

- ⇨ Dokumentation schriftlicher Einwilligungen, von Verpflichtungen auf das Datenschutzgeheimnis, des Berechtigungskonzepts
- ⇨ Überprüfung der Verarbeitung von personenbezogenen Daten im Ausland
- ⇨ Überprüfung der Auftragsdatenverarbeitung und Anpassung der zugehörigen Verträge
- ⇨ Mithilfe zur Umsetzung der Datenschutzrichtlinien für neue IT-Beschaffungsmaßnahmen
- ⇨ Erstellung eines Verfahrensverzeichnisses
- ⇨ Beantworten von Datenschutzanfragen
- ⇨ usw.

Der externe Datenschutzbeauftragte

Vorteile – 1

- ⇨ Weisungsfreiheit besser gewährleistet, als beim Teilzeit DSB (Laufzeit ~ 3 – 5 Jahre)
- ⇨ Tatsächlich unabhängig im Sinne des BDSG
- ⇨ Unterliegt nicht dem Betriebsrat
- ⇨ Externe DSB hat neutrale Stellung und wird als Autorität eher anerkannt von
  - ➲ Geschäftsleitung
  - ➲ Betriebsrat
- ⇨ Mehr Möglichkeiten der Fortbildung ➔bessere Qualifizierung
- ⇨ Keine internen Aus- und Weiterbildungskosten

Der externe Datenschutzbeauftragte

Vorteile – 2

- ⇨ Zeitbudget nicht von anderen Aufgaben eingeschränkt
- ⇨ Effektiverer Ressourceneinsatz
- ⇨ Nicht betriebsblind
- ⇨ Aktuelles Know-how, da davon unabhängig ⇨ bessere Akzeptanz als fachliche Autorität
- ⇨ Professionelle Umsetzung des Datenschutz-Managements
- ⇨ Verbesserung der strategischen Unternehmensposition
- ⇨ Minderung des Haftungsrisikos der Geschäftsführung
- ⇨ Problemlose Kündigung möglich

Datenschutz: So nicht!

Graphik: BSI

Alle Fehler gefunden?

Graphik
BSI

Auflösung

1. Türen und Fenster stehen offen: Rechner und Zubehör könnten aus den Räumen gestohlen werden.
2. Der Bildschirm und damit möglicherweise auch vertrauliche Informationen können von Unbefugten eingesehen werden.
3. Ein Zettel mit Passwörtern ist sichtbar und könnte von Unbefugten missbraucht werden.
4. Eine mit "Sicherung" beschriftete CD-ROM liegt zugänglich herum.
5. Ausdrucke und Kopien mit vermutlich vertraulichen Daten liegen an Druckern und Kopierern.
6. Rechner mit direkter Verbindung an das Internet können den zentralen Firewallschutz des Netzes aushebeln.
7. Durch private Datenträger (im Bild eine CD-ROM) kann Schadsoftware Icon Glossar ungeprüft in das Unternehmensnetz gelangen.
8. Austretende Flüssigkeiten gefährden die Hardware.
9. Rauchen bedeutet Brandgefahr. (Quelle: BSI)

Noch Fragen zum Thema Datenschutz?

RE Engineering und Consulting
Ralf Essl
Geprüfter Datenschutzbeauftragter (FH)
Hochalmstraße 5
81825 München

Telefon 089-43749909
Telefax 089-43749910
E-Mail ralf.essl@dsb-group.de
und info@essl-consult.de
Internet www.essl-consult.de
und www@dsb-group.de

„Ulmer Modell“
Das Ulmer Urteil zur Fachkunde
Landgericht Ulm (Az.: 5T 153/90-01 LG Ulm)

Das Landgericht Ulm hat in seinem als "Ulmer Urteil" in die Rechtsgeschichte eingegangenen Beschluss festgestellt, dass betriebliche und behördliche Datenschutzbeauftragte einen Beruf ausüben. Weil sie mit ihrer Tätigkeit einen auf Dauer berechneten und nicht vorübergehenden Beitrag zur gesellschaftlichen Gesamtleistung erbringen. Auch wenn sie ihre Aufgabe als Datenschutzbeauftragte neben ihrem eigentlichen Hauptberuf ausüben, sei diese Tätigkeit aus verfassungsrechtlicher Sicht als Beruf anzusehen.

Zwar mache nach Auffassung des Ulmer Landgerichts das Bundesdatenschutzgesetz (BDSG) die Tätigkeit als Datenschutzbeauftragte(r) nicht von einem bestimmten Ausbildungsgang abhängig. Dennoch sprechen zahlreiche Einzelregelungen des Gesetzes für das Vorliegen eines relativ konkreten Berufsbildes:

"Dem Datenschutzbeauftragten kommt in öffentlichen Einrichtungen, der Wirtschaft, der Industrie und bei den Behörden in heutiger Zeit **ein wichtiger Auftrag für die Wahrung der Belange der Gesellschaft** zu. Seine Aufgabe besteht darin, Beeinträchtigungen und Gefahren entgegenzuwirken, die sich aus dem massenhaften Umgang mit Daten und Informationen ergeben, die über bestimmte Personen gespeichert sind. Es liegt auf der Hand, dass hierdurch die Persönlichkeitsrechte des einzelnen Bürgers in erheblichem Maße beeinträchtigt und tangiert sein können."

Im Anschluss daran führt das Ulmer Landgericht aus, dass Datenschutzbeauftragte die Aufgabe haben, "... für die Wahrung des Persönlichkeitsrechts im Rahmen der geltenden Gesetze Sorge zu tragen. Bei der Erfüllung dieser öffentlichen Aufgaben ist er nicht an Weisungen des Arbeitgebers gebunden. Das Gesetz verlangt von ihm die erforderliche Fachkunde und Zuverlässigkeit. Gerade **an seine Fachkunde werden hohe Anforderungen gestellt**."

Zur Fachkunde stellte das Ulmer Landgericht fest, dass die Anforderungen an den Datenschutzbeauftragten, der Computerexperte sein soll/muss, mindestens folgende Punkte umfassen:

- Anwendung der Vorschriften der Datenschutzgesetze des Bundes und der Länder und alle anderen den Datenschutz betreffenden Rechtsvorschriften
- Kenntnisse der betrieblichen Organisation
- didaktische Fähigkeiten
- psychologisches Einfühlungsvermögen
- Organisationstalent
- angemessener Umgang in Konflikten um seine Person, seine Funktion und seine Aufgabe