

**Prüfungsfragen zur schriftlichen VWA-Diplom-Prüfung „Datenschutz“ (Hund)**

13. Studiengang Informatik-Betriebswirt SS 2003

Maximale Punktzahl: 60 Punkte

1. Nennen Sie bitte vier wesentliche Meilensteine in der Entwicklung der Datenschutz-Gesetzgebung.

**Lösung (3 Punkte):**

- 1977 bis 1979 sukzessives Inkrafttreten von BDSG und LDSG
- 1983 Volkszählungsurteil des BVerfG (Recht auf informationelle Selbstbestimmung)
- 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität
- 1991 Novelle des Bundesdatenschutzgesetzes
- 1995 neue EU-Datenschutzrichtlinie
- 1996/97 Telegesetze (TKG, lUKDG)
- 2001 Novelle des Bundesdatenschutzgesetzes (1. Stufe)
- 12.11.2001 Vorlage eines Gutachtens zur 2. Stufe der Novellierung des BDSG
- 21.12.2001 Novellierung des Teledienstedatenschutzgesetzes
- 31.07.2002 EU-Datenschutzrichtlinie für elektronische Kommunikation

2. Unter welchen gesetzlichen Voraussetzungen ist die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten nach dem BDSG zulässig?

**Lösung (6 Punkte):**

**Die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten ist zulässig, sofern**

- eine andere Rechtsvorschrift außerhalb des BDSG dies erlaubt oder anordnet ✓
- der Betroffene eingewilligt hat ✓
- eine Vorschrift des BDSG dies erlaubt oder anordnet.

3. Was besagt nach dem BDSG der Subsidiaritätsgrundsatz?

**Lösung (3 Punkte):**

**Soweit andere Rechtsvorschriften auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften des BDSG vor.**

4. Gibt es beim Schadenersatz Unterschiede zwischen dem öffentlichen und dem nicht-öffentlichen Bereich, und wenn ja, welche?

**Lösung (6 Punkte):**

Ja, es gibt Unterschiede.

**a) Beim öffentlichen Bereich**

- verschuldensunabhängiger Schadenersatz bei unzulässiger oder unrichtiger Erhebung, Verarbeitung und Nutzung
- Schmerzensgeld auch für immaterielle Schäden bei schwerer Verletzung des Persönlichkeitsrechts
- Begrenzung auf vormals DM 250.000,00
- gesamtschuldnerische Haftung
- weitergehende Ersatzansprüche sowie Gerichtsweg möglich.

**b) Im nicht-öffentlichen Bereich Verschuldenshaftung mit Beweislastumkehr.**

5. Datengeheimnis § 5 BDSG

- a) Was besagt die Vorschrift des § 5 BDSG (Datengeheimnis)?  
 b) Gibt es Unterschiede zwischen dem öffentlichen und nicht-öffentlichen Bereich?  
 c) Kennen Sie neben dem Datengeheimnis noch andere Geheimnisse oder Verschwiegenheitspflichten, die ein Unternehmen ggf. zu beachten hat, und wenn ja, welche?

**Lösung\*(9 Punkte):**

- a) Personenbezogene Daten dürfen nicht unbefugt verarbeitet oder genutzt werden. Die Verarbeitung der Daten ist auf das notwendige Maß zu beschränken, das durch die rechtmäßige Aufgabenerfüllung gesetzt ist. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort. *+ Verpflichtung zum DG bei nichtöffentl. Stellen =*
- b) Ja, im Gegensatz zum öffentlichen Bereich ist im nicht-öffentlichen Bereich eine ausdrückliche Verpflichtung der Mitarbeiter vorgeschrieben.
- c) Weitere Verschwiegenheitspflichten oder Geheimnisse, die vom Mitarbeiter oder dem Unternehmen einzuhalten sind: berufliche Verschwiegenheitspflichten, betriebliche Schweige- und Geheimhaltungspflichten, Brief- und Fernmeldegeheimnis.

## 6. Vorabkontrolle

- a) Wann muss eine Vorabkontrolle im Sinne des § 4d Abs. 5 vorgenommen werden?
- b) Welche Ausnahmen von der Vorabkontrolle gibt es?
- c) Welche Rolle spielt der DSB bei der Vorabkontrolle?

**Lösung (9 Punkte):**

- a) **Soweit automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, ist eine Vorabkontrolle durchzuführen. Dies gilt insbesondere bei der Verarbeitung besonders sensibler Daten (§ 3 Abs. 9) oder wenn die Verarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.**
- b) **Ausnahmen:  
Wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.**
- c) **Bei Pflicht zur Vorabkontrolle ist immer ein DSB zu bestellen. Dieser ist auch für die Durchführung der Vorabkontrolle zuständig.**

*Zweifels*

7. Datentransfer ins Ausland (§§ 4b und 4c)

Ein deutsches Unternehmen mit Zweigniederlassung in Italien beabsichtigt, Personal-  
daten eines in die italienische Niederlassung versetzten Mitarbeiters dorthin zu trans-  
ferieren.

- a) Müssen bei dieser Datenübermittlung gleiche Vorschriften wie zwischen inländischen Stellen beachtet werden?
- b) Gilt für die geplante Datenübermittlung deutsches (BDSG) oder italienisches Recht?
- c) Welches Recht (deutsches oder italienisches Recht) ist zu beachten, wenn die Daten von der italienischen Niederlassung weiterverarbeitet werden?
- d) Wäre ein Datentransfer unter gleichen Voraussetzungen möglich, wenn der Sitz der Niederlassung nicht in Italien, sondern in einem Drittstaat außerhalb der EU gelegen wäre?

**Lösung ( 12 Punkte):**

- a) Nein, für Datenübermittlungen innerhalb der EU gelten gleiche Vorschriften wie zwischen inländischen Stellen.**
- b) Für die geplante Datenübermittlung gilt deutsches Recht und damit das BDSG (Sitzlandprinzip).**
- c) Wegen des Sitzlandprinzips gilt italienisches Recht, da die Daten in Italien verarbeitet werden.**
- d) Nein, da beim Datentransfer in Drittstaaten außerhalb der EU erschwerte Voraussetzungen (z. B. Prüfung des angemessenen Datenschutzniveaus, Genehmigung durch Aufsichtsbehörde) zu beachten ist.**

## 8. Datensicherheit (§ 9 BDSG)

- a) Was besagt der Verhältnismäßigkeitsgrundsatz des § 9 BDSG?
- b) Nennen Sie bitte neben der Zugangskontrolle noch 4 weitere der insgesamt 8 Kontrollarten der Anlage zu § 9 BDSG.
- c) Welche der 8 Kontrollarten müssen bei der Karteiverarbeitung (nicht automatisierte Datenverarbeitung) beachtet werden?
- d) Welche rechtlichen Konsequenzen ergeben sich, wenn ein Verarbeitungsvorhaben nicht hinreichend abgesichert werden kann?

**Lösung (12 Punkte):**

- a) **Erforderlich sind Datensicherungsmaßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.**
- b) **Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle**
- c) **Keine, da die Anlage zu § 9 nur für die automatisierte Verarbeitung, nicht aber für die – nicht automatisierte – Karteiverarbeitung gilt.**
- d) **Die Verarbeitung wäre unzulässig und daher zu unterlassen.**