Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 1. Übung im SoSe 2009:
BDSG (1)

1.1 BDSG-Rechtsgrundlagen für Aktiengesellschaften

Aufgabe:

- Welche Abschnitte aus dem BDSG sind für Aktiengesellschaften relevant? Begründen Sie Ihre Antwort!

1.1 BDSG-Rechtsgrundlagen für Aktiengesellschaften (1)

Abgrenzung:

Aktiengesellschaften = Kapitalgesellschaften = Gesellschaft des privaten Rechts
→ **nicht-öffentliche Stelle** nach § 2 Abs. 4 BDSG

Relevante Abschnitte für nicht-öffentliche Stellen im BDSG:

- 1. Abschnitt: Allgemeine und gemeinsame Bestimmungen
  = §§ 1 – 11 BDSG (samt Anlage zu § 9 Satz 1 BDSG)
- 3. Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen
  = §§ 27 – 38a BDSG
- 4. Abschnitt: Sondervorschriften
  = §§ 39 – 42 BDSG
- 5. Abschnitt: Schlussvorschriften
  = §§ 43 – 44 BDSG
- 6. Abschnitt: Übergangsvorschriften
  = §§ 45 – 46 BDSG

1.1 BDSG-Rechtsgrundlagen für Aktiengesellschaften (2)

Begründung:

- Lediglich der 2. Abschnitt (Datenverarbeitung der öffentlichen Stellen) ist nicht für Aktiengesellschaften relevant, da diese nicht unter die betreffende Kategorie fallen (siehe Abgrenzung)
- Die allgemeinen Vorschriften weisen keine Einschränkungen bei der Gültigkeit auf, so dass sämtliche Paragraphen insbesondere auch für nicht-öffentliche Stellen wie Aktiengesellschaften gelten, sofern die jeweiligen Einzelvoraussetzungen erfüllt sind (was z.B. bei § 4b BDSG unzutreffend ist, wenn die betreffende Aktiengesellschaft keine personenbezogenen Daten ins Ausland übermittelt).
- Die Abschnitte 4 bis 6 sind analog zu betrachten. Allerdings ist der 4. Abschnitt i.d.R. für Aktiengesellschaften unzutreffend, sofern diese nicht gerade mit einem Berufsgeheimnis (z.B. Steuerberater, Wirtschaftsprüfer, Rechtsanwälte oder Ärzte etc. gemäß § 203 StGB) oder einem Amtsgeheimnis (sofern durch gesetzliche Regelung „beliehen“, d.h. mit einer hoheitlichen Funktion ausgestattet) zu tun haben (eher unwahrscheinlich!).

1.2 Voraussetzungen zur automatisierten DV

Aufgabe:

- Wann ist eine automatisierte Datenverarbeitung personenbezogene Daten bei einer GmbH zulässig? Gibt es hier Unterschiede in Abhängigkeit zur Art der personenbezogenen Daten? Begründen Sie Ihre Antwort!

Hinweis:

- *Automatisierte Datenverarbeitung = Erhebung, Verarbeitung oder Nutzung unter Einsatz einer Funktionseinheit zur Datenverarbeitung (DV-Anlage)*

1.2 Voraussetzungen zur automatisierten DV (1)

Abgrenzung:
GmbH = Kapitalgesellschaft = Gesellschaft des privaten Rechts
→ **nicht-öffentliche Stelle** nach § 2 Abs. 4 BDSG

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, soweit (nach § 4 Abs. 1 BDSG):

- das BDSG dies erlaubt oder anordnet,
- eine andere Rechtsvorschrift dies erlaubt oder anordnet,
- oder der Betroffene eingewilligt hat.

→ Verbot mit Erlaubnisvorbehalt!

1.2 Voraussetzungen zur automatisierten DV (2)

Gestattungsnormen bei **nicht-öffentlichen Stellen**:

- zur Erfüllung eigener Geschäftszwecke (§ 28 Abs. 1 BDSG), wenn
  - es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient
  - es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und diesem keine schutzwürdigen Interessen des Betroffenen entgegenstehen
  - die Daten allgemein zugänglich sind
- für anderen Zweck unter Abwägung (§ 28 Abs. 2 BDSG)
- zur Übermittlung oder Nutzung für anderen Zweck gemäß Katalog aus § 28 Abs. 3 BDSG: Wahrung berechtigter Interessen, Gefahrenabwehr, Strafverfolgung, Werbung bei Listenprivileg unter Abwägung oder zur wissenschaftlichen Forschung

1.2 Voraussetzungen zur automatisierten DV (3)

Aber: Besondere Vorschriften für Umgang mit **besonderen Arten personenbezogener Daten** (gem. § 3 Abs. 9 BDSG = Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben)
→ **es gibt Unterschiede in Abhängigkeit zur Art der personenbezogenen Daten**:

- bei nicht-öffentlichen Stellen nach § 28 Abs. 6 BDSG zum Schutz lebenswichtiger Personeninteressen, bei vom Betroffenen offenkundig öffentlich gemachten Daten, zur Rechtsdurchsetzung unter Abwägung sowie zur wissenschaftlichen Forschung und nach § 28 Abs. 7 BDSG zur medizinischen DV

1.3 Einwilligungserklärung

Aufgabe:

- Welchen Anforderungen muss eine Einwilligung nach den Vorschriften des BDSG genügen? Begründen Sie Ihre Antwort! Nennen Sie zudem Fälle, wo es fragwürdig ist, ob diese Anforderungen wirklich erfüllt sind!

1.3 Einwilligungserklärung (1)

Anforderungen an eine Einwilligungserklärung:

- Einwilligung nur wirksam, wenn aufgrund **freier Entscheidung** des Betroffenen erfolgt (§ 4a Abs. 1 Satz 1 BDSG)
- **Verwendungszweck** ist anzugeben (§ 4a Abs. 1 Satz 2 BDSG)
- **Schriftform** i.d.R. erforderlich (§ 4a Abs. 1 Satz 3 BDSG)
- Einwilligung muss **gut erkennbar** sein (§ 4a Abs. 1 Satz 4 BDSG)
- Bei **besonderen Arten personenbezogener Daten** muss dies **ausdrücklich erklärt** werden (§ 4a Abs. 3 BDSG)

1.3 Einwilligungserklärung (2)

Fragwürdige Einwilligungserklärungen:

- Kopplung der Einwilligung an andere Leistungen
- Belohnung der Einwilligung durch Geschenke oder Vergünstigungen
- Einwilligung in unbestimmte Zwecke
- Einwilligung in beliebige Zweckänderungen
- Einwilligung in Verzicht auf Betroffenenrechte
- Einwilligung ohne Aufklärung über Folgen
- Einwilligung in umfassende AGBs ohne Abänderbarkeit
- Einwilligung in beliebige Weiterübermittlung
- Einwilligung in umfangreiche Erhebungen bei Bewerbungen bzw. Beschäftigungs-/Dienstantritt

1.4 Einwilligungserklärungsmuster

Aufgabe:

- Formulieren Sie eine Einwilligungserklärung, die alle Anforderungen nach dem BDSG erfüllt, anhand eines frei gewählten Beispiels!

1.4 Einwilligungserklärungsmuster

Muster einer Einwilligungserklärung:

Hiermit willige ich ein, dass die unten aufgeführten personenbezogenen Daten von der <Bezeichnung der verantwortlichen Stelle> zum Zweck der <Zweck> erhoben, verarbeitet und genutzt werden dürfen. Ich wurde darüber informiert, dass ich diese Einwilligung jederzeit ohne Nachteile widerrufen kann. Von der <Bezeichnung der verantwortlichen Stelle> wurde mir versichert, dass meine datenschutzrechtlichen Belange ohne Einschränkung gewährleistet werden und keine Übermittlung meiner Daten an Dritte erfolgt.

1.5 Prüfkriterien zum Datenschutzniveau: Unternehmen

Aufgabe:

- Anhand welcher Prüfkriterien, basierend auf den Bestimmungen aus dem BDSG, kann man das Datenschutzniveau eines Unternehmens beurteilen? Begründen Sie Ihre Antwort unter Angabe der Rechtsquellen!

1.5 Prüfkriterien zum Datenschutzniveau: Unternehmen (1)

- Unternehmen = nicht-öffentliche Stelle

→ Vorhandensein und Angabentiefe eines Verfahrensverzeichnisses [§ 4g Abs. 2 BDSG]

→ Hinweis zur Rechtsgrundlage für die jeweilige Datenverarbeitung (Rechtsvorschrift oder Einwilligungserklärung) [§ 4 Abs. 1 BDSG]

→ Vorliegen einer informierten Einwilligungserklärung [§ 4a BDSG]

→ Umsetzung der Betroffenenrechte [§§ 33 – 35 BDSG i.V.m. § 6 BDSG]

→ ggf. Bestellung eines Datenschutzbeauftragten [§ 4f BDSG]

→ Veröffentlichtes Ergebnis eines Datenschutzaudits [§ 9a BDSG] – *Hinweis: Ausführungsgesetz fehlt noch!*

1.5 Prüfkriterien zum Datenschutzniveau: Unternehmen (2)

→ Meldung/Bericht der Aufsichtsbehörde über festgestellte Datenschutzverstöße [§ 38 Abs. 1 BDSG]
Hinweis: <u>geplant</u> ist im Rahmen der nächsten BDSG-Novelle(n) eine Meldung der verantwortlichen Stelle an die Betroffenen bei Feststellen eines Datenverlusts!

→ Überprüfung der technischen und organisatorischen Maßnahmen (z.B. durch Dritte im Rahmen eines Datenschutz-Audits) [§ 9 BDSG samt Anlage]

→ Einhaltung der Datensparsamkeit [§ 3a BDSG]