Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2008:
BDSG (2) & Kundendatenschutz (1)

2.1 Prüfkriterien zum Datenschutzniveau: Unternehmen

- Unternehmen = nicht-öffentliche Stelle

→ Zulässigkeitsüberprüfung der Datenverarbeitung (Rechtsvorschrift oder Einwilligungserklärung) [§ 4 Abs. 1 BDSG]

→ Überprüfung der technischen und organisatorischen Maßnahmen [§ 9 BDSG samt Anlage]

→ Einhaltung der Datensparsamkeit [§ 3a BDSG]

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

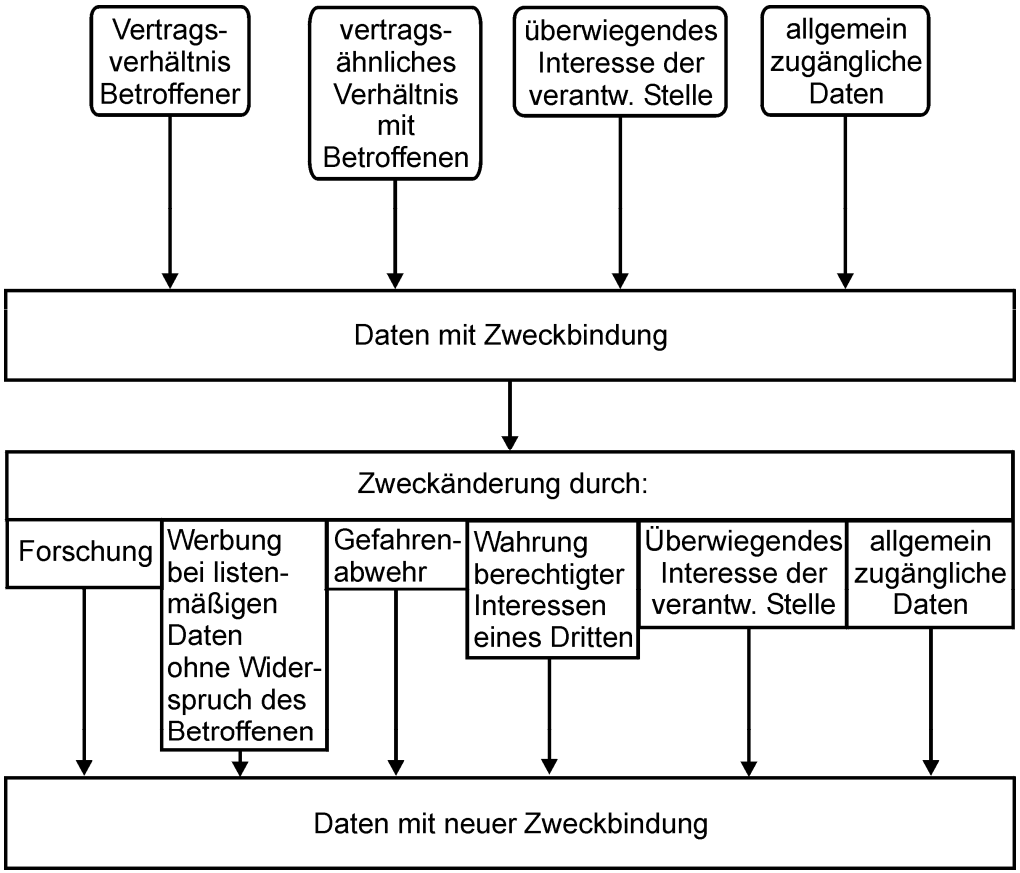
→ Bestellung eines Datenschutzbeauftragten [§ 4f BDSG]

→ Audit von Datenschutzkonzept & technischen Einrichtungen [§ 9a BDSG] – *Hinweis: Ausführungsgesetz fehlt noch!*

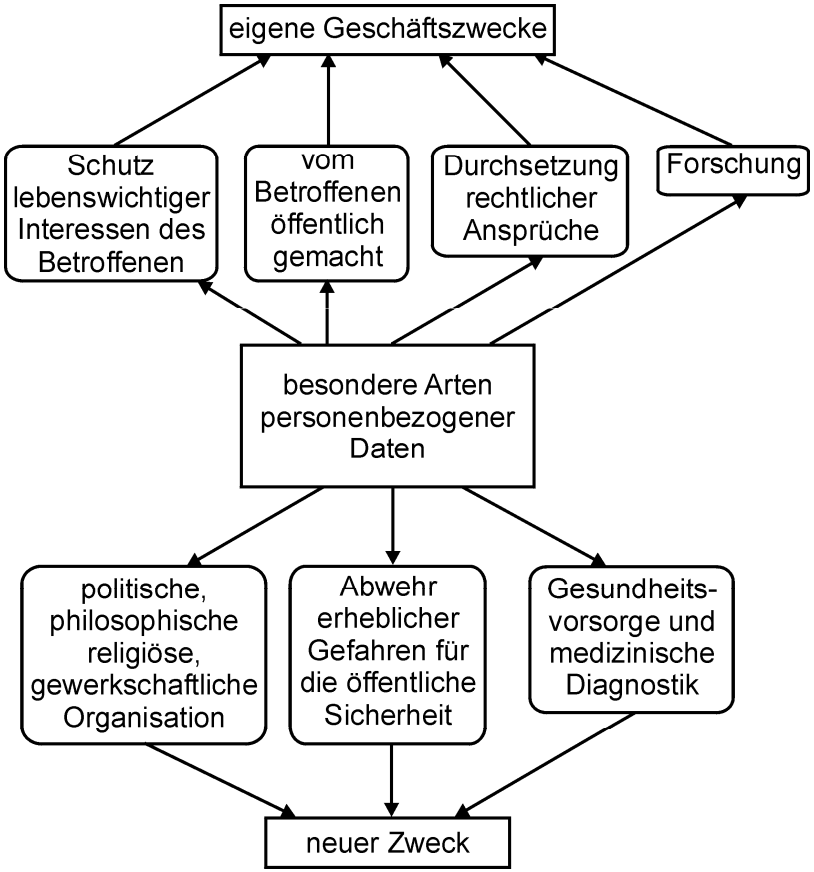
2.1 Prüfkriterien zum Datenschutzniveau: Kunde

- → Vorhandensein und Angabentiefe eines Verfahrensverzeichnisses [§ 4g Abs. 2 BDSG]
- → Hinweis zur Rechtsgrundlage für die Kundendatenverarbeitung (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!*
- → Meldung/Bericht der Aufsichtsbehörde [§ 38 Abs. 1 BDSG]

2.2 Schema zu § 28 BDSG (1)



2.2 Schema zu § 28 BDSG (2)



2.3 besondere Arten personenbezogener Daten (1)

- besondere Arten personenbezogener Daten in § 3 Abs. 9 BDSG definiert; automatisierte Verarbeitung in § 3 Abs. 2 BDSG
- jede automatisierte Verarbeitung ist nur zulässig, wenn eine Rechtsnorm dies erlaubt bzw. anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG)
- bei der Rechtsgrundlage einer Einwilligung ist auf den Umstand der Erhebung, Verarbeitung oder Nutzung besonderer Arten personenbezogener Daten ausdrücklich hinzuweisen (§ 4a Abs. 3 BDSG)

2.3 besondere Arten personenbezogener Daten (2)

- automatisierte Verarbeitungen besonderer Arten pesonenbezogener Daten weisen u.U. besondere Risiken für die Rechte und Freiheiten der Betroffenen auf und unterliegen daher der Vorabkontrolle (§ 4d Abs. 5 BDSG)
- die Vorabkontrolle wird durch den Datenschutzbeauftragten durchgeführt (§ 4d Abs. 6 BDSG); hierzu ist dem Datenschutzbeauftragten das Verfahrensverzeichnis samt einer Aufstellung der geplanten Zugriffsberechtigungen auszuhändigen

2.3 besondere Arten personenbezogener Daten (3)

- Personen, die mit der automatisierten Verarbeitung besonderer Arten personenbezogener Daten befasst sind, sind auf das Datengeheimnis zu verpflichten (§ 5 BDSG)
- die Betroffenenrechte auf Auskunft, Berichtigung, Löschung oder Sperrung sind in jedem Falle im vollen Umfang zu gewährleisten (§ 6 Abs. 1 BDSG)
- eine automatisierte Einzelentscheidung ist bei der automatisierten Verarbeitung besonderer Arten personenbezogener Daten unzulässig (§ 6a Abs. 1 BDSG)

2.3 besondere Arten personenbezogener Daten (4)

- eine unzulässige automatisierte Verarbeitung besonderer Arten personenbezogener Daten verpflichtet zum Schadensersatz, wenn die verantwortliche Stelle nicht nachweisen kann, dass sie ihrer Sorgfaltspflicht nachgekommen ist (§ 7 BDSG)
- zum Schutz der besonderen Arten personenbezogener Daten sind die erforderlichen technischen und organisatorischen Maßnahmen zu treffen (§ 9 BDSG)

2.3 besondere Arten personenbezogener Daten (5)

- soll die automatisierte Verarbeitung besonderer Arten personenbezogener Daten in Form eines automatisierten Abrufverfahrens erfolgen, ist nachzuweisen, dass dies unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen angemessen ist (§ 10 Abs. 1 BDSG) und schriftliche Angaben zu machen, aus denen u.a. auch die technischen und organisatorischen Maßnahmen zum Datenschutz ausgeführt werden (§ 10 Abs. 2 BDSG – also nicht nur eine allgemeine Beschreibung wie beim internen Verfahrensverzeichnis)

2.3 besondere Arten personenbezogener Daten (6)

- soll die automatisierte Verarbeitung besonderer Arten personenbezogener Daten durch einen Auftragnehmer erfolgen, bleibt der Auftraggaber verantwortliche Stelle (§ 11 Abs. 1 BDSG) und hat einen Auftragnehmer insbesondere aufgrund der dort getroffenen technischen und organisatorischen Maßnahmen auszusuchen (§ 11 Abs. 2 BDSG); ggf. kann er hierzu dem Auftragnehmer Weisungen erteilen (§ 11 Abs. 3 BDSG)
- zu den spezifischen Anforderungen aus § 28 Abs. 6 – 9 BDSG siehe 2.2 Teil 2

2.3 besondere Arten personenbezogener Daten (7)

- wenn die Korrektheit besonderer Arten personenbezogener Daten nicht durch die verantwortliche Stelle bewiesen werden kann, sind diese zu löschen (§ 35 Abs. 2 Nr. 2 BDSG); eine Sperrung reicht jedoch aus, wenn eine Löschung mit einem unverhältnismäßig hohem Aufwand möglich wäre (§ 35 Abs. 3 Nr. 3 BDSG)

2.4 Verfahrensverzeichnis für Kundendatenverwaltung (1)

1. Name oder Firma der verantwortlichen Stelle:
   Kundendata GmbH & Co. KG
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen:
   Geschäftsführer: Peter Müller
   Vertriebsleiter: Josef Schmidt
   EDV-Leiterin: Andrea Schulze

2.4 Verfahrensverzeichnis für Kundendatenverwaltung (2)

3. Anschrift der verantwortlichen Stelle:
   Kundendata GmbH & Co. KG
   Musterstr. 1
   12345 Musterstadt
4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung:
   Kundendatenverwaltung
5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien:
   Betroffene: Kunden der Kundendata GmbH & Co. KG
   Datenkategorien: Kontaktdaten, Vertragsdaten

2.4 Verfahrensverzeichnis für Kundendatenverwaltung (3)

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:
   Inkassounternehmen bei Zahlungsverzug
   öffentliche Stellen aufgrund gesetzlicher Vorgaben
   interne Stellen (Finanzbuchhaltung) zur Aufgabenerfüllung
7. Regelfristen für die Löschung der Daten:
   6 Jahre
8. eine geplante Datenübermittlung in Drittstaaten:
   entfällt

2.4 Verfahrensverzeichnis für Kundendatenverwaltung (4)

9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind: [nicht öffentlich!]

- Gebäude nur mittels Chipkartenfreischaltung betretbar
- Datenserver in besonders geschütztem Serverraum gespeichert, zu dem nur EDV-Personal Zutritt hat
- Datensätze werden täglich auf Band gesichert, das im Tresor aufbewahrt wird (anderer Brandabschnitt)

2.4 Verfahrensverzeichnis für Kundendatenverwaltung (5)

9. Fortsetzung

- Rückeinspielung von Bandsicherungen auch im Notfall erprobt
- Kundendatenverwaltungsprogramm erfordert Anmeldung am System mittels Kennung und Passwort, sowie einer benutzerbezogenen Kennwort-Eingabe
- Passwort weist ausreichende Komplexität auf (8 Stellen, Angabe von Buchstaben, Zeichen und Sonderzeichen obligatorisch)
- Zugriffsberechtigt sind nur befugte Benutzer

2.5 Kundendatenanalyse (1)

- Kundendatenverwaltung unterliegt Zweckbindung, bei der Datenerhebung ist daher auf den Zweck der Werbung hinzuweisen (§ 28 Abs. 1 BDSG)
- Unternehmen hat berechtigtes Interesse daran, seine Kunden (auf der Grundlage der bestehenden Vertragsbeziehung) zielgerichtet bewerben zu wollen (§ 28 Abs. 1 Nr. 2 BDSG)
- sofern die Kunden nicht einer Bewerbung widersprochen haben, dürfen diese auch beworben werden; andernfalls sind deren Daten zu sperren (§ 28 Abs. 4 BDSG)

2.5 Kundendatenanalyse (2)

- die Einrichtung der Datenbank zur Kundendatenanalyse ist zulässig nach § 4 BDSG, da abgesichert aufgrund des bestehenden Vertragsverhältnisses nach § 28 Abs. 1 BDSG
- bei der Einrichtung der Datenbank sind die entsprechenden Datenschutzvorschriften (insb. hinsichtlich der technischen und organisatorischen Maßnahmen nach § 9 BDSG) einzuhalten und das mit der Kundendatenanalyse befasste Personal auf das Datengeheimnis zu verpflichten (§ 5 BDSG)

2.5 Kundendatenanalyse (3)

- da verschiedene Datensätze zielgerichtet auswertet werden sollen, um insb. entsprechende Kaufprofile zu ermitteln, sind besondere Risiken für die Betroffenen im Zuge einer Vorabkontrolle auszuschließen (§ 4d Abs. 5 BDSG)
- Weitergabe anonymisierter Kundendatenanalysen an „vergleichbare Kunden“ (stellen dabei Dritte dar!) nur nach ausdrücklicher Trennung von Identifikationsmerkmalen zulässig (§ 30 Abs. 1 BDSG)