Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2012:
Kundendatenschutz (1)

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke

Aufgabe:

- Beschreiben Sie anhand der Ausführungen in § 28 BDSG, was ein Unternehmen beachten muss, wenn es personenbezogene Daten
  a) zum Zweck der Vertragserfüllung bzw.
  b) zum Zweck der Werbung
  automatisiert verarbeiten möchte!

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (1)

a) Automatisierte Verarbeitung zur Vertragserfüllung
   → Vertrag = rechtsgeschäftliches Schuldverhältnis
   → Zweck der Vertragserfüllung = eigener Geschäftszweck

Vorgaben aus § 28 BDSG für DV zur Vertragserfüllung:

- § 28 I BDSG relevant für Erheben, Verarbeiten (ohne Sperren & Löschen!) und Nutzen von personenbezogenen Daten zur Erfüllung eigener Geschäftszwecke
- DV zulässig, wenn dies für Begründung, Durchführung oder Beendigung eines Vertrags mit dem Betroffen erforderlich ist (§ 28 I Nr. 1 BDSG)

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (2)

a) Vorgaben aus § 28 BDSG zur Vertragserf. (1. Forts.):

→ Unternehmen muss Erforderlichkeitsprüfung durchführen, d.h. positiv feststellen, dass der Zweck nicht ohne eine entsprechende DV erfüllbar ist (auf der Grundlage einer Prozessanalyse)

- DV auch zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass diesem schutzwürdige Betroffeneninteressen entgegen stehen (§ 28 I Nr. 2 BDSG)

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (3)

a) Vorgaben aus § 28 BDSG zur Vertragserf. (2. Forts.):

→ DV ggf. im Rahmen einer Abwägung zulässig
→ berechtigte Interessen müssen nachweisbar sein
→ DV muss für berechtigte Interessen erforderlich sein
→ Betroffeneninteressen sind ausdrücklich den berechtigten Interessen gegenüberzustellen

- DV von Daten, die allgemein zugänglich sind, sofern diesem nicht schutzwürdige Interessen des Betroffenen offensichtlich überwiegt (§ 28 I Nr. 3 BDSG)
  → im Zweifel also kein Ausschlussgrund!

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (4)

a) Vorgaben aus § 28 BDSG zur Vertragserf. (3. Forts.):

- Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (§ 28 I Satz 2 BDSG)
  → konkreter Vertragserfüllungszweck vorrangig
  → sollen Nebenzwecke (z.B. Werbung) ebenfalls erfüllt werden, muss dies angegeben werden
  → selbst bei berechtigten Interessen sind etwaige Zwecke nachvollziehbar festzulegen
- Alternative aus § 28 II BDSG hier (!) nicht relevant

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (5)

b) Automatisierte Verarbeitung zur Werbung
→ vorrangige Regelungen in § 28 III BDSG

Vorgaben aus § 28 BDSG für DV zur Werbung:

- DV zum Zweck der Werbung zulässig, soweit der Betroffene eingewilligt hat (§ 28 III Satz 1 BDSG)
  → wenn keine schriftliche Einwilligung vorliegt, reicht auch eine elektronische Einwilligung nach § 28 IIIa BDSG (entsprechend zu § 13 II TMG) bzw. eine schriftliche Bestätigung des Inhalts an den Betroffenen (Grundlage für Widerspruchsrecht aus § 28 IV BDSG)

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (6)

b) Vorgaben aus § 28 BDSG zur Werbung (1. Forts.):

- Werbung zudem zulässig, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt (z.B. Bestandskunden!), sofern die DV erforderlich ist
  → neben Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel, akademischer Grad, Anschrift und Geburtsjahr (sofern diese Daten direkt beim Betroffenen erhoben wurden) dürfen weitere Daten hinzugespeichert werden (§ 28 III S. 3 BDSG)
  → Rechtsgrundlage für CRM-System!

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (7)

b) Vorgaben aus § 28 BDSG zur Werbung (2. Forts.):

- Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen zulässig an dessen berufliche Anschrift (§ 28 III Nr. 2 BDSG)
- Werbung, die nicht auf der Grundlage einer Einwilligung erfolgt, erfordert Abwägung
  → Der Datenverwendung dürfen keine schutzwürdigen Interessen des Betroffenen entgegenstehen (§ 28 III S. 6 BDSG)
  → Ausschlussgrund wäre z.B. unlautere Werbung

2.1 Kundendatenverarbeitung für eigene Geschäftszwecke (8)

b) Vorgaben aus § 28 BDSG zur Werbung (3. Forts.):

- Unternehmen hat Widerspruchsrecht des Betroffenen zu beachten, da dann ein Verarbeiten oder Nutzen der Daten unzulässig ist (§ 28 IV Satz 1 BDSG)
- Betroffene ist bei der Ansprache zum Zweck der Werbung über die verantwortliche Stelle sowie über sein Widerspruchsrecht zu unterrichten (§ 28 IV Satz 2 BDSG)

2.2 Kundenspezifische Datenanalysen

Aufgabe:

- Ein Unternehmen möchte ein datenschutzkonformes Customer-Relationship-Management-System (CRM-System) einführen. In diesem CRM-System sollen alle kundenspezifische Daten zusammengetragen werden, die das Unternehmen bereits in verschiedenen Quellen gespeichert hat. Zu den Kunden zählen ausschließlich Privatpersonen. **Wie muss das Unternehmen hierzu vorgehen?** Begründen Sie Ihre Antwort!

2.2 Kundenspezifische Datenanalysen (1)

- Unternehmen = nicht-öffentliche Stelle
- CRM-System = System zur Kunden**bewertung**
  → Vorabkontrolle erforderlich (§ 4d V BDSG)
  → Vorabkontrolle durch DSB (§ 4d VI BDSG)
  → DSB muss bestellt sein / werden (§ 4f I BDSG)
- Hinsichtlich der vorgesehenen DV prüfen, ob jeweilige Zweckfestlegung (nach § 28 I Satz 2 BDSG) die geplante Zusammenlegung gestattet und hierfür ein berechtigtes Interesse vorliegt (§ 28 II BDSG i.V.m. § 28 I Nr. 2 BDSG)
  → Nachweis für Erforderlichkeit & Abwägung

2.2 Kundenspezifische Datenanalysen (2)

- Durchführende Beschäftigte sind auf das Datengeheimnis zu verpflichten (§ 5 BDSG)
- Für das CRM-System sind ausreichende technische und organisatorische Maßnahmen zu ergreifen (§ 9 BDSG samt Anlage)
- CRM-System stellt eigenes Verfahren im Verfahrensverzeichnis dar

2.3 Verfahren beim Kundendatenschutz

Aufgabe:

- Ein Unternehmen betreibt hinsichtlich des Umgangs mit Kundendaten folgende technischen Systeme:
  - Web-Portal zur Erhebung von Bestellwünschen,
  - ERP-System zur Verfolgung des Herstellungsprozesses bestellter Güter und der Verwaltung der Finanzströme,
  - CRM-System zur Datenpflege der Kundenbeziehungen
  - sowie ein Lagerverwaltungs-System zur Steuerung, Zwischenlagerung und Bereitstellung für den Versand hergestellter Güter mittels RFID-Chips.

  Welche datenschutzrechtlichen Verfahren hinsichtlich der Kundendatenverarbeitung erkennen Sie anhand dieser Beschreibung?

2.3 Verfahren beim Kundendatenschutz (1)

Kundendatenschutzrechtliche Verfahren sind hier:

- Web-Portal zur Erhebung von Bestellwünschen, da der Kunde seine Identifikationsdaten angeben muss, um später die Bestellung überhaupt zugesandt bekommen zu können
- ERP-System zur Verwaltung der Finanzströme, da nach Versand der Bestellung (und der zugehörigen Rechnungsstellung!), die Eingänge von Überweisungen bzw. Barzahlungen (z.B. gegen Nachnahme) zu überwachen sind
  → ERP-System-Teil zur Buchhaltung
- CRM-System zur Datenpflege der Kundenbeziehungen, da hierin die komplette Kundenhistorie abgelegt wird

→ Obige Systeme sind zugleich als Verfahren anzusehen

2.3 Verfahren beim Kundendatenschutz (2)

Anmerkungen:

- *Die Verfolgung des Herstellungsprozesses bestellter Güter mittels des ERP-Systems ist aufgrund der damit durchgeführten Betriebsdaten-erfassung ein mitarbeiterdatenschutzrechtliches Verfahren*
- *Das Lagerverwaltungs-System zur Steuerung, Zwischenlagerung und Bereitstellung für den Versand hergestellter Güter mittels RFID-Chips kann ggf. ebenfalls als mitarbeiterdatenschutzrechtliches Verfahren angesehen werden, wenn z.B. aufgrund innerbetrieblicher Aufgabenzu-weisungen durch die Überwachung der RFID-Chips zugleich eine Mit-arbeiterüberwachung (Bewegungsprofil!) möglich ist; für den Fall, dass die RFID-Chips nicht bei der Bereitstellung zum Versand deaktiviert werden, kann es sein, dass der Empfänger durch die Nutzung der mit dem RFID-Chip versehenen Güter selbst ein Persönlichkeitsprofil of-fenbart (Bewegung & Kaufverhalten)*

2.4 Datenschutzrisiko gemäß Vorabkontrolle

Aufgabe:

- Für ein geplantes Kundenbetreuungsverfahren (alle Kunden sind Endverbraucher) mittels Web-Portal wurden seitens des Vertriebs folgende Wünsche formuliert:
  - ° Das Web-Portal soll auf die Kundendaten des CRM-Systems automatisiert zugreifen können (sowohl lesend als auch schreibend)
  - ° Die Kunden sollen eine fortlaufende Nummer als Benutzerkennung erhalten und das Web-Portal nach Eingabe eines frei gewählten Passwortes nutzen können
  - ° Für durchgeführte Bestellungen sollen die Kunden eine Bestätigungsmail erhalten
  - ° Im Web-Portal sollen die Kunden ihre Bestellhistorie einsehen können
- Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer Vorabkontrolle (gem. § 4d Abs. 5 BDSG) sehen, schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß angefügter 5x5-Risk-Map. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

2.4 Datenschutzrisiko gemäß Vorabkontrolle (1)

A) Ermittlung potenzieller Datenschutzrisiken:

- Lesender & schreibender Zugriff des Web-Portals auf CRM-System
  1. Unbeschränkter Zugriff auf alle CRM-Daten
  2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben
- Benutzerkennung via fortlaufender Nummer & freie Passwortwahl
  3. Enumerative Zugangsdaten
  4. Mangelnder Zugriffsschutz bei geringer Passwortgüte
- Bestätigungsmail für durchgeführte Bestellungen
  5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
- Einsicht in Bestellhistorie via Web-Portal
  6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil

Bei 1., 2., 5. und 6. unmittelbarer Zugriff auf personenbezogenen Daten

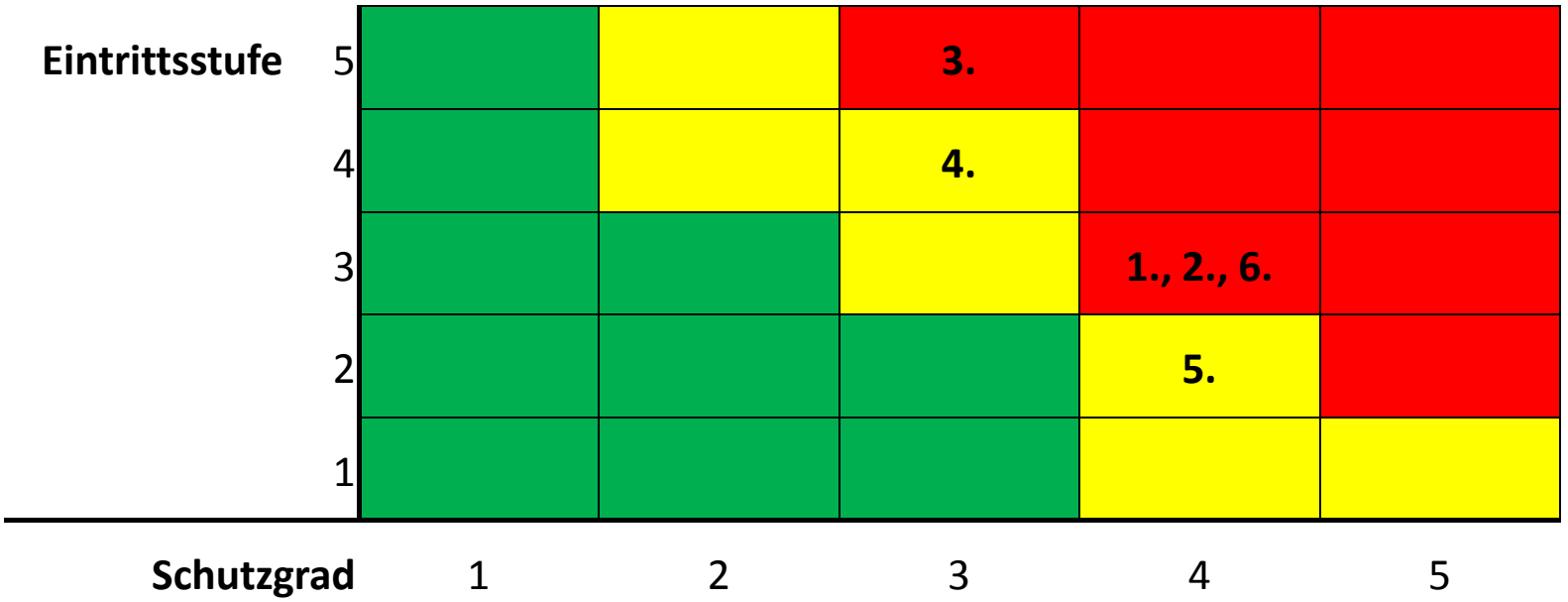
→ Schutzgrad 4; bei 3. und 4. dagegen Schutzgrad 3 (Pseudonym)

2.4 Datenschutzrisiko gemäß Vorabkontrolle (2)

B) Abschätzung der Eintriffsstufe:

1. Unbeschränkter Zugriff auf alle CRM-Daten: 3, da Angreifer über begrenzte Fähigkeiten & Ressourcen verfügen muss, um Daten z.B. via SQL-Injection abrufen zu können
2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben: 3, da ebenfalls via SQL-Injection
3. Enumerative Zugangsdaten: 5, da Ausprobieren voraussetzungslos
4. Mangelnder Zugriffsschutz bei geringer Passwortgüte: 4, da Passwort-Cracker leicht downloadbar sind & schlechte Passwörter i.d.R. bereits leicht zum Erfolg führen (z.B. Benutzerkennung = Passwort)
5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden: 2, da Verbindungspfad erst ermittelt werden muss
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil: 4, wg. 3. & 4.

2.4 Datenschutzrisiko gemäß Vorabkontrolle (3)



Rot = Aktivität nötig; **Gelb** = Aktivität prüfen; **Grün** = Akzeptabel

2.4 Datenschutzrisiko gemäß Vorabkontrolle (4)

C) Handlungsempfehlung:

1. Unbeschränkter Zugriff auf alle CRM-Daten
   → Datenvalidierung sicherstellen
2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben
   → Schreibenden Zugriff auf CRM unterbinden
3. Enumerative Zugangsdaten
   → Benutzerkennung frei wählen lassen
4. Mangelnder Zugriffsschutz bei geringer Passwortgüte
   → Mindestvorgaben für Passwortgüte festlegen
5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
   → ggf. akzeptierbar
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil
   → nach Änderung zu 3. & 4. ggf. akzeptierbar

2.5 Weitergabe von Zahlungsverzugsdaten

Aufgabe:

- **Wie** muss ein Unternehmen **vorgehen**, wenn es aufgrund ausstehender Zahlungseingänge
  a) diese Forderungen an ein Inkassounternehmen bzw.
  b) entsprechende Zahlungsverzugsdaten an eine Auskunftei
  übertragen möchte? Begründen Sie Ihre Antwort!

2.5 Weitergabe von Zahlungsverzugsdaten (1)

a) Datenweitergabe an Inkassounternehmen

- Inkassounternehmen = Dritte
  → **Forderungs**übertragung erfordert Datenübertragung (berechtigte Interessen des Dritten nach § 28 II Nr. 2 lit. a BDSG)
  → Datenweitergabe = Übermittlung (gem. § 3 IV Nr. 3 lit. a BDSG)
  → Dateneinsicht = Übermittlung (gem. § 3 IV Nr. 3 lit. b BDSG)
  → Inkassounternehmen verfolgt anschließend eigene Zwecke mit übermittelten Daten

2.5 Weitergabe von Zahlungsverzugsdaten (2)

a) Datenweitergabe an Inkassounternehmen (Forts.)

- Betroffene ist wahlweise vom Inkassounternehmen bei der erstmaligen Speicherung der übermittelten Daten zu benachrichtigen (§ 33 I BDSG), sofern er nicht bereits auf andere Weise davon Kenntnis erlangt hat (§ 33 II Nr. 1 BDSG)
  → üblich: Forderungsabtretung an Inkassobüro entweder in AGB oder in Mahnung ankündigen
- Bei Datenübermittlung ist insb. auf Verschlüsselung zu achten (neben üblichen Vorkehrungen nach §§ 5 & 9 BDSG)

2.5 Weitergabe von Zahlungsverzugsdaten (3)

b) Datenweitergabe an Auskunftei

- Für **Daten**übermittlung an Auskunftei § 28a BDSG vorrangig!
- Datenübermittlung nur zulässig, wenn geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist
  → ausstehender Zahlungseingang muss fällig sein
  → keine per-se-Datenübermittlung zulässig!
- Für Datenübermittlung müssen berechtigte Interessen der verantwortlichen Stelle oder eines Dritten vorliegen

2.5 Weitergabe von Zahlungsverzugsdaten (4)

b) Datenweitergabe an Auskunftei (1. Forts.)

- Für die Forderung muss ein durchsetzbarer Titel (§ 28a I Nr. 1 BDSG), Insolvenzrelevanz (§ 28a I Nr. 2 BDSG) oder ausdrückliche Anerkennung durch den Betroffenen (§ 28a I Nr. 3 BDSG) vorliegen oder der Betroffene nach Eintritt der Fälligkeit mind. 2x schriftlich gemahnt worden sein, zwischen der ersten Mahnung und der Übermittlung wenigstens 4 Wochen liegen, der Betroffene vor der Übermittlung, aber nicht vor der ersten Mahnung informiert worden sein, ohne dass der Betroffene die Forderung bestritten hat (§ 28a I Nr. 4 BDSG), oder der zugrunde liegende Vertrag aufgrund der Zahlungsrückstände fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat (§ 28a I Nr. 5 BDSG)

2.5 Weitergabe von Zahlungsverzugsdaten (5)

b) Datenweitergabe an Auskunftei (2. Forts.)

- Sollte sich an den Tatsachen, die für die Übermittlung ausschlaggebend waren, etwas geändert haben, muss die verantwortliche Stelle dies der Auskunftei mitteilen (§ 28a III BDSG)
- Auch hier muss bei der Übermittlung darauf geachtet werden, dass die Daten nicht unbefugt durch Dritte eingesehen werden können (→ Verschlüsselung) neben den üblichen Vorkehrungen (§§ 5 & 9 BDSG)