Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2011:
Kundendatenschutz (2)

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 (Fortbestand des Listenprivilegs), sofern die DV erforderlich ist
  → neben Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel, akademischer Grad, Anschrift und Geburtsjahr (gemäß Listenprivileg) auch Daten aus allgemein zugänglichen Adress-, Rufnummern-, Brachen- oder vergleichbaren Verzeichnissen hinzufügbar (§ 28 III Nr. 1 BDSG)

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)
- Übermittlungssondervorschriften hier (!) nicht relevant, da Werbung für eigene Zwecke oder für fremde Angebote (bei Letzterem muss für den Betroffenen bei der Ansprache die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar sein (§ 28 III Satz 5 BDSG)

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 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? Welche technischen und organisatorischen Maßnahmen sind für die von Ihnen erkannten Verfahren zwingend, damit keine besonderen Risiken für die Rechte und Freiheiten der Betroffenen davon ausgehen können? Begründen Sie Ihre Antwort!

2.2 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

2.2 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)*

2.2 Verfahren beim Kundendatenschutz (3)

Schutz des Web-Portals (= Kundengewinnungsverfahren):

- Zuverlässiges Authentifizierungsverfahren
- Opt-in-Lösung für Bestellungen zur Kontrolle für Betroffenen
- Manipulationsschutz für Eintragungen mittels Datenvalidierung & Vergabe restriktiver Schreibrechte
- Keine Upload-Funktion, um Malware-Einspeisung zu verhindern
- Redundante Technik zur Ausfallsicherheit des Portals
- Protokollierung der Datenübertragung (z.B. ans ERP-System) im Rahmen der Bestellabwicklung, wobei eine unmittelbare Übertragung vom Web-Portal ins LAN vorzugsweise zu vermeiden ist (Holsystem statt Bringsystem)

2.2 Verfahren beim Kundendatenschutz (4)

Schutz des Buchhaltungssystems (= Kundenbetreuungsverfahren):

- Wirksamer Zugriffsschutz
- Einsatz eines geeigneten Benutzerrollenkonzepts, da ERP-System auch andere Funktionen erfüllt
- Protokollierung von Eingaben, Veränderungen & Löschungen, um kompletten Prozess nachweisen zu können
- Besonderes Augenmerk auf ggf. bestehende Schnittstellen zur Kontenverwaltung (Online-Banking bzw. eCash-Verwaltung, sofern vorgesehen – dann ergänzende Anforderungen bei Web-Portal wg. Bank-/Kreditkartendateneingabe!)
- Protokollierung der Datenübertragung (z.B. ans CRM-System) im Rahmen der Überwachung der Kundenhistorie

2.2 Verfahren beim Kundendatenschutz (5)

Schutz des CRM-Systems (= Kundenbindungsverfahren):

- Gewährleistung der Zweckbindung
- Wirksamer Zugriffsschutz (i.d.R. andere Zugriffsberechtigte als beim Buchführungssystem wg. Segregation of Duties!)
- Bereitstellung von anonymisierten Reports (→ Vermeidung von Drill-Down-Funktionen)
- Regelmäßige Kontrollen, ob eine unzulässige Datenanreicherung stattfand
- Protokollierung über Anfertigung spezifischer Auswertungen & Beschränkung möglicher Auswertungsfunktionen
- Sperrfeld zur Berücksichtigung von Werbewidersprüchen

2.3 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!

2.3 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

2.3 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)

2.3 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

2.3 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)

2.3 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)

2.4 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!

2.4 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

2.4 Kundenspezifische Datenanalysen (2)

- Durchführende Beschäftigte sind auf das Datenge-heimnis 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 Verfahrens-verzeichnis dar

2.5 Geschäftsmäßige Datenübermittlung

Aufgabe:

- Darf ein Unternehmen Kundendatenanalysen unter Einbeziehung soziodemographischer Daten (vor allem hinsichtlich der Kaufkraft und Bonität) von Wohngebieten erstellen und diese Dritten geschäftsmäßig übermitteln? Begründen Sie Ihre Antwort!

2.5 Geschäftsmäßige Datenübermittlung (1)

- Die Auswertung von Kundendaten unter Einbeziehung sozio-demographischer Daten von Wohngebieten (vor allem hinsichtlich Kaufkraft und Bonität) stellt ein Verfahren dar, das dazu bestimmt ist, die Persönlichkeit der Betroffenen (hier: Kunden) zu bewerten → **Vorabkontrolle nach § 4d Abs. 5 BDSG erforderlich!**
- Die Daten werden geschäftsmäßig zum Zweck der Übermittlung gespeichert, so dass das Verfahren der Aufsichtsbehörde nach § 4d Abs. 4 BDSG zu melden ist.

2.5 Geschäftsmäßige Datenübermittlung (2)

- Nach § 29 Abs. 1 BDSG ist die geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung nur zulässig, wenn
  - ° der Betroffene kein Ausschluss geltend machen kann und
  - ° die Daten aus allgemein zugänglichen Quellen stammen.

  Anm.: Der Verweis auf § 28a BDSG ist hier nicht relevant.

  → soziodemographische Daten der Wohngebiete können zwar aus anonymisierten Untersuchungen stammen, doch werden diese mit den Kundendaten lt. Aufgabe verknüpft (= **Scoring**!)
- Für Scoring-Daten ist § 28b BDSG zu beachten, sofern dieses (datenschutzrechtlich eigenständiges!) Verfahren der Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen dient

2.5 Geschäftsmäßige Datenübermittlung (3)

- Für Scoring-Verfahren dürfen nur wissenschaftlich anerkannte mathematisch-statistische Verfahren verwendet werden (§ 28b Nr. 1 BDSG)
  → vorausgesetzt, für das Vorhaben wird auf ein entsprechendes Verfahren zurückgegriffen, bestehen insoweit keine Einwände
- Bei der Berechnung des Wahrscheinlichkeitswertes für ein bestimmtes zukünftiges Verhalten des Betroffenen dürfen nicht ausschließlich Anschriftendaten genutzt werden (§ 28b Nr. 3 BDSG)
  → da laut Aufgabenstellung Anschriftendaten mit soziodemographischen Daten kombiniert werden sollen, resultiert daraus kein Ausschlussgrund
- Der Betroffene ist nachweisbar über die Verwendung seiner Anschriftendaten zu unterrichten (§ 28b Nr. 4 BDSG)
  → nach Aufgabenstellung unklar, ob diese Unterrichtung erfolgte

2.5 Geschäftsmäßige Datenübermittlung (4)

- Die Übermittlung der Scoring-Daten darf nach § 29 Abs. 2 BDSG nur erfolgen, wenn
  - ° der empfangende Dritte ein berechtigtes Interesse geltend machen kann (ist z.B. bei Auskunfteien wie Schufa zur Identifizierung kreditunwürdiger Personen gegeben)
    - – nach Aufgabenstellung hier nicht zwingend gegeben
  - ° und der Betroffene kein Ausschluss geltend machen kann
    - – nach Aufgabenstellung nicht entscheidbar, da unklar ist, welchen Schutzbedarf die zu nutzenden Daten aufweisen

  → Abwägung über damit verbundene Risiken aber erforderlich

  → Abwägungsergebnis ist zu dokumentieren (§ 29 Abs. 2 Satz 3 BDSG)

  → positive Gestattung insoweit nicht eindeutig konstatierbar

2.5 Geschäftsmäßige Datenübermittlung (5)

- Nach der Aufgabenstellung wurden die Betroffenen nicht ausdrücklich auf diese Kundendatenanalyse unter Einbeziehung von Scoring-Daten hingewiesen, was aber bei der Übermittlung erforderlich ist (§ 29 Abs. 2 Satz 3 BDSG i.V.m. § 28b Nr. 4 BDSG)

→ Voraussetzungen des § 29 BDSG nicht erfüllt!

→ **Geschäftsmäßige Übermittlung unzulässig!**
(Ergebnis der Vorabkontrolle)