Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2010:

BDSG (2) & Kundendatenschutz (1)

2.1 Verfahrensverzeichnis für Kundendatenverwaltung

Aufgabe:

- Erstellen Sie anhand der Auflistung aus § 4e BDSG ein sog. "Verfahrensverzeichnis", das jeder einsehen darf, für die Kundendatenverwaltung eines Unternehmens!

Anmerkung:

- „Kundendatenverwaltung“ ist ggf. bei Unternehmen zu unspezifisch, wenn z.B. ein CRM-System, ein ERP-System und BI-System im Einsatz ist

2.1 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

2.1 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

2.1 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 Aufgaben-erfüllung
7. Regelfristen für die Löschung der Daten:
   6 Jahre (Geschäftsbriefe), 10 Jahre (Buchungsdaten)
8. eine geplante Datenübermittlung in Drittstaaten:
   entfällt

2.1 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!**
   → nicht Bestandteil des Verfahrensverzeichnisses, das jeder einsehen darf (§ 4g Abs. 2 Satz 2 BDSG)

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung

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!

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (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)

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (2)

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

→ DV muss zur Vertragserfüllung erforderlich sein

→ 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)

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (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!

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (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)
  → Vertragserfüllungszweck muss eindeutig sein
  → 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

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (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)

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (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)

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (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)

2.2 DV zur Vertragserfüllung bzw. zur Kundenbewerbung (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)

2.3 Umgang mit besonderen Arten personenbezogener Daten

Aufgabe:

- Was hat ein Unternehmen nach dem BDSG zu beachten, wenn es im Rahmen der Kundendatenverarbeitung besondere Arten personenbezogener Daten automatisiert zu verarbeiten hat? Begründen Sie Ihre Antwort!

2.3 Umgang mit besonderen 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 Umgang mit besonderen 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 Umgang mit besonderen 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 Umgang mit besonderen 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 Umgang mit besonderen 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 Umgang mit besonderen Arten personenbezogener Daten (6)

- soll die automatisierte Verarbeitung besonderer Arten personenbezogener Daten durch einen Auftragnehmer erfolgen, bleibt der Auftraggeber 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)
- Außerdem sind die spezifischen Anforderungen aus § 28 Abs. 6 – 9 BDSG zu beachten (vorrangige Vorschriften!)

2.3 Umgang mit besonderen Arten personenbezogener Daten (7)

- Sofern der Betroffene nicht nach Maßgabe des § 4a Abs. 3 BDSG eingewilligt hat, ist dies zulässig:
  - ° zum Schutz lebenswichtiger Interessen, wenn der Betroffene selbst nicht einwilligen kann (§ 28 VI Nr. 1 BDSG)
  - ° wenn der Betroffene diese Daten offenkundig öffentlich gemacht hat (§ 28 VI Nr. 2 BDSG)
  - ° zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche, soweit erforderlich & bedeutender als das Betroffeneninteresse (§ 28 VI Nr. 3 BDSG)
  - ° zur wissenschaftlichen Forschung (§ 28 VI Nr. 4 BDSG)

2.3 Umgang mit besonderen Arten personenbezogener Daten (8)

- Zum Zweck der Gesundheitsvorsorge, medizinischen Diagnostik, Gesundheitsversorgung oder Behandlung bzw. für die Verwaltung von Gesundheitsdiensten, sofern erforderlich & durch Personen mit ärztlicher Schweigepflicht durchgeführt (§ 28 VII BDSG)
- Politische, philosophische, religiöse o. gewerkschaftlich ausgerichtete Organisationen dürfen Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakt unterhalten, automatisiert verarbeiten, sofern sie keinen Erwerbszweck verfolgen (§ 28 IX BDSG)

2.3 Umgang mit besonderen Arten personenbezogener Daten (9)

- Übermittlung zu anderem Zweck (§ 28 VIII BDSG) hier (!) nicht relevant
- 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 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!

2.4 Weitergabe von Zahlungsverzugsdaten (1)

a) Datenweitergabe an Inkassounternehmen

- Inkassounternehmen = Dritte
  → Forderungsübertragung 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

2.4 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)

2.4 Weitergabe von Zahlungsverzugsdaten (3)

b) Datenweitergabe an Auskunftei

- Für Datenübermittlung 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

2.4 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)

2.4 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)

2.5 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!

2.5 Kundenspezifische Datenanalysen (1)

- Unternehmen = nicht-öffentliche Stelle
- CRM-System = System zur Kundenbewertung
  → 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

2.5 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