Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2009:
BDSG (2) & Kundendatenschutz (1)

2.1 Schema zu § 28 BDSG

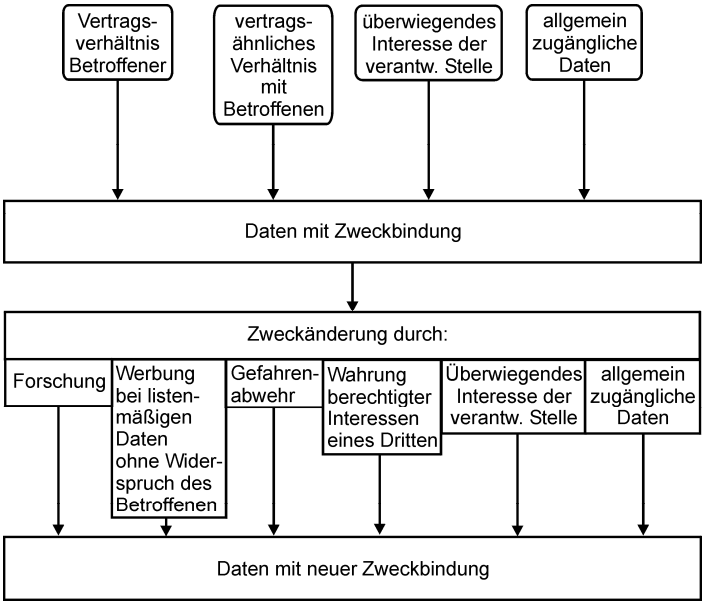
Aufgabe:

- Erstellen Sie ein Schema zu § 28 BDSG, aus der hervorgeht, wann eine Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke einer Offenen Handelsgesellschaft zulässig ist!

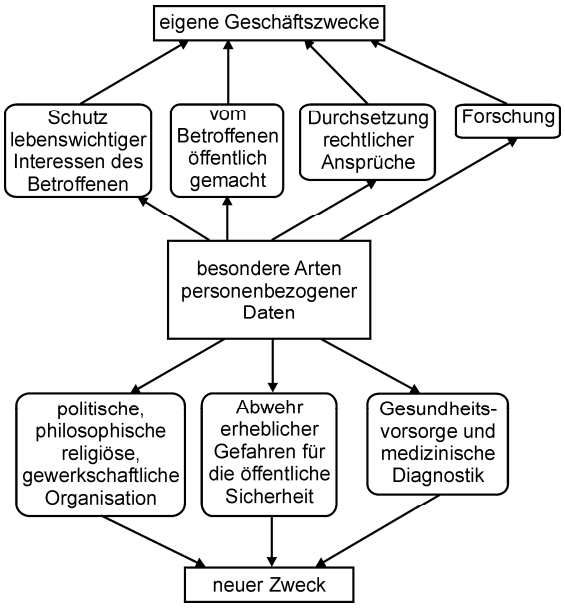
<u>Anmerkung:</u>

- OHG = Personengesellschaft = nicht-öffentliche Stelle
  → § 28 BDSG für OHG relevant.

2.1 Schema zu § 28 BDSG (1)



2.1 Schema zu § 28 BDSG (2)



2.2 Umgang mit besonderen Arten personenbezogener Daten

Aufgabe:

- Beschreiben Sie anhand der Vorschriften aus dem BDSG, was ein Unternehmen zu beachten hat, wenn es besondere Arten personenbezogener Daten automatisiert zu verarbeiten hat!

2.2 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)

2.2 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

2.2 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)

2.2 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)

2.2 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)

2.2 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)
- zu den spezifischen Anforderungen aus § 28 Abs. 6 – 9 BDSG siehe 2.1 Teil 2!

2.2 Umgang mit besonderen 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)

2.3 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

2.3 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

2.3 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

2.3 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 (Geschäftsbriefe), 10 Jahre (Buchungsdaten)
8. eine geplante Datenübermittlung in Drittstaaten:
   entfällt

2.3 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)

2.4 Kundendatenanalyse

Aufgabe:

- Wie muss ein Unternehmen vorgehen, wenn es zur Kundendatenanalyse eine Datenbank erstellen möchte, mit deren Hilfe Kunden gezielt in den Konsumbereichen beworben werden sollen, in denen sie entweder bereits Artikel erstanden haben, oder für solche Artikel (auch in anderen Konsumbereichen) gewonnen werden sollen, die von "vergleichbaren" Kunden gekauft wurden?

2.4 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)

2.4 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)

2.4 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)

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 soziodemographischer 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 nicht aus allgemein zugänglichen Quellen stammen.

  → soziodemographische Daten der Wohngebiete können zwar aus anonymisierten Untersuchungen stammen, doch werden diese mit den Kundendaten lt. Aufgabe verknüpft (= Scoring)

2.5 Geschäftsmäßige Datenübermittlung (3)

- Scoring-Daten dürfen nach § 29 Abs. 2 BDSG nur übermittelt werden, 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
  - ° oder es sich um listenmäßig zusammengefasste Daten handelt zum Zweck der Werbung oder Markt- / Meinungsforschung
    – nach Aufgabenstellung hier nicht zwingend gegeben
  - ° und der Betroffene kein Ausschluss geltend machen kann
  - → Abwägung über damit verbundene Risiken erforderlich
  - → positive Gestattung nicht eindeutig konstatierbar

2.5 Geschäftsmäßige Datenübermittlung (4)

- Nach der Aufgabenstellung wurden die Betroffenen nicht ausdrücklich auf diese Kundendatenanalyse unter Einbeziehung von Scoring-Daten hingewiesen, was aber bei der Übermittlung zugunsten von Werbung oder Markt-/Meinungsforschung erforderlich wäre nach § 29 Abs. 4 BDSG i.V.m. § 28 Abs. 4 BDSG
- Das berechtigte Interesse der empfangenden Stelle wäre von der übermittelnden Stelle nach § 29 Abs. 2 Satz 3 BDSG glaubhaft aufzuzeichnen, was nicht aus der Aufgabenstellung hervorgeht.

→ Voraussetzungen des § 29 BDSG nicht erfüllt!

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