Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2009:
Kundendatenschutz (3)

4.1 Nutzungsprofile

Aufgabe:

- Darf ein Provider vorhandene Nutzungsinformationen seiner Kunden zu einem nutzerbezogenen Persönlichkeitsprofil zusammentragen? Begründen Sie Ihre Antwort unter Nennung der entsprechenden Rechtsquellen!

4.1 Nutzungsprofile

- Eine Providingtätigkeit fällt unter das Telemedienrecht. Sofern die telemedienrechtlichen Bestimmungen für die Beantwortung der Frage nicht ausreichen, ist das BDSG subsidiär heranzuziehen, da es ebenfalls um personenbezogene Daten im zugrunde liegenden Fall geht.
- Nach § 15 III TMG darf ein Dienstanbieter zum Zweck der Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der angebotenen Telemedien Nutzungsprofile unter Verwendung von Pseudonymen erstellen, sofern der Nutzer diesem nicht widerspricht. Auf sein Widerspruchsrecht ist der Nutzer im Rahmen der Datenschutzerklärung hinzuweisen. Die Nutzungsprofile dürfen nicht mit den Daten über den jeweiligen Träger des Pseudonyms zusammengeführt werden.
- Eine nutzungsbezogene Zusammenstellung von Nutzungsprofilen ist also zulässig, nicht jedoch eine personenbezogene Zusammenstellung! **Die Erstellung eines nutzerbezogenen Persönlichkeitsprofils ist folglich unzulässig**, sofern der Kunde nicht (zumindest indirekt) eingewilligt hat.
- Ein Rückgriff auf das BDSG ist damit nicht mehr erforderlich.

4.2 angereichertes CRM-System

Aufgabe:

- Von einem Unternehmen soll ein Auftragnehmer damit beauftragt werden, Datenmaterial über strukturelle Erkenntnisse zusammenzustellen, die sich aus den bestehenden Kundendaten des verwendeten CRM-System ergeben. Diese sollen angereichert werden mit soziodemographischen Merkmalen (vor allem Kaufkraft der jeweiligen Wohngegend) und über Lebensverhältnisse der Kunden (Familienstand, Hobbies, Bonität). Führen Sie hierzu eine Vorabkontrolle durch und begründen Sie Ihr Ergebnis unter Nennung der entsprechenden Rechtsquellen!

4.2 angereichertes CRM-System (1)

- Ein Customer-Relationship-Management-System (CRM-System) beschreibt, in welcher Beziehung das Unternehmen zu ihren Kunden (& Interessenten) steht.
- Ein CRM-System dient daher der Bewertung der Persönlichkeit der Betroffenen (im Sinne eines Persönlichkeitsprofils), weshalb dieses bei Einrichtung einer Vorabkontrolle nach § 4d V Nr. 2 BDSG zu unterziehen ist. Der laufende Betrieb darf ebenfalls keine besonderen Risiken für die Rechte und Freiheiten der Betroffenen zur Folge haben.
- Bei der Tätigkeit eines Auftragnehmers ist nach § 11 II BDSG sicherzustellen, dass dieser über ausreichende technische und organisatorische Schutzmaßnahmen verfügt und insbesondere die Zweckbindung und Datentrennung im Rahmen des Berechtigungskonzepts gemäß der Anlage zu § 9 BDSG gewährleistet.
- Nach der Aufgabenstellung sollen die bestehenden CRM-Datensätze angereichert werden um soziodemographische Merkmale (Kaufkraft der Wohngegend) und Daten über die Lebensverhältnisse der Kunden (Familienstand, Hobbies, Bonität).

4.2 angereichertes CRM-System (2)

- Die Anreicherung selbst stellt damit eine erhebliche Erweiterung des bestehenden CRM-Systems dar und bedarf daher ebenfalls der Vorabkontrolle!

1. Prüfung der Rechtmäßigkeit im Rahmen der Vorabkontrolle:

- Erkenntnisse über die Kaufkraft von Wohngebieten können aus hinreichend anonymisierten Studien bzw. statistischen Erhebungen gewonnen werden, die frei bezogen werden können. Ein Unternehmen kann insbesondere aufgrund der Art ihres Geschäftsfeldes ein berechtigtes Interesse nach § 28 I Nr. 2 BDSG i.d.R. nachweisen, dass damit auf die Auftragstätigkeit aufgrund der Bindungswirkung aus § 11 I BDSG ausstrahlt. Die Aufgabenstellung ergibt hier noch keinen zwingenden Grund, warum diese Anreicherung unzulässig sein sollte, zumal auch kein Hinweis vorliegt, aus dem sich ein überwiegendes Interesse der Betroffenen am Ausschluss dieser Anreicherung ergibt.
- Gleiches gilt für die Angabe der Bonität, da ein Anbieter dazu berechtigt ist, seine Lieferungen und Leistungen nur an Kunden abzugeben, die dazu (ggf. durch Kreditgewährung) in der Lage sind, die Lieferungen und Leistungen auch zu bezahlen.

4.2 angereichertes CRM-System (3)

- Angaben über den Familienstand können i.d.R. aus allgemein zugänglichen Daten gewonnen werden, da diese i.d.R. im jeweiligen Amtsblatt veröffentlicht werden. Dennoch ist hier bereits fraglich, ob dieses Datum noch in Beziehung zum eigentlichen Vertragsverhältnis gesetzt werden kann.
- Die Angabe der Hobbies hingegen kann in keinem Fall aus entsprechenden Quellen gewonnen werden und spätestens hier ergibt sich auch ein höher zu gewichtendes Interesse der Betroffenen am Ausschluss einer entsprechenden Anreicherung! [Auch wenn dies in der Praxis immer wieder anzutreffen ist!]
- Insgesamt wird folglich bei der geplanten Anreicherung des bestehenden CRM-Systems die Persönlichkeit der Betroffenen in besonders intensiver Weise abgebildet (quantitativ & qualitativ), so dass diese nicht mehr beeinflussen können, ob ihr informationelles Selbstbestimmungsrecht noch angemessen gewahrt wird. **Die geplante Anreicherung (im Zuge einer Auftragsdaten-verarbeitung) ist folglich unzulässig!**

→ **Insofern kann eine Festlegung zu treffender Schutzvorkehrungen unterbleiben, da bereits an dieser Stelle die Vorabkontrolle terminiert.**

4.3 CRM-Zugriff d. ext. Call-Center

Aufgabe:

- Ein Unternehmen bietet seinen Kunden das Hosting von Web-Seiten an. Unter den Kunden befinden sich überwiegend Privatpersonen. Der Vertrag wird elektronisch im Internet geschlossen unter Einhaltung des double-opt-in-Verfahrens. Das Unternehmen möchte nun seine Kunden durch einen externen Call-Center über die Zufriedenheit mit dem bereitgestellten Web-Service befragen. Darf das Call-Center auf das CRM-System des Unternehmens zugreifen? Begründen Sie Ihre Antwort!

4.3 CRM-Zugriff d. ext. Call-Center (1)

Eingrenzung:

- **Hosting von Web-Seiten**
  → Telemedienrecht anzuwenden → § 5 TMG (allgemeine Informationspflichten), §§ 7 II und 10 TMG (Haftungserleichterung hinsichtlich der gespeicherten Web-Seiten-Inhalte der Kunden), § 12 TMG (Grundsätze), § 13 TMG (Pflichten des Diensteanbieters), § 14 TMG (Bestandsdaten), § 15 TMG (Nutzungsdaten)
  → Kunden **überwiegend Privatpersonen** → ggf. BDSG subsidiär zu TMG (1. & 3. Abschnitt des BDSG, da Hosting-Anbieter eine nicht-öffentliche Stelle ist)
- Vertragsabschluss im Internet mittels double-opt-in
  → § 13 II TMG
- **externer Call-Center**
  → Auftragsdatenverarbeitung (§ 11 BDSG) oder Funktionsübertragung (§ 28 BDSG)
  → Anruf durch Call-Center → Fernmeldegeheimnis (§ 88 TKG), Call-Center hat angemessene Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten zu treffen (§ 109 I Nr. 1 TKG)

4.3 CRM-Zugriff d. ext. Call-Center (2)

Aufgrund fehlender Angabe in Aufgabe → **Fallunterscheidung**:

1. Call-Center mittels Auftragsdatenverarbeitung beauftragt:

- Bei einer Auftragsdatenverarbeitung nach § 11 II BDSG ist sicherzustellen, dass der Auftragnehmer über ausreichende technische und organisatorische Schutzmaßnahmen verfügt.
- Die Auftragstätigkeit muss nach § 11 II BDSG präzise schriftlich festgelegt worden sein. Dies betrifft auch etwaige Unterauftragsverhältnisse.
- Call-Center folglich als Verlängerung der verantwortlichen Stelle anzusehen, so dass **gegen den Zugriff auf das CRM-System durch den Call-Center keine grundsätzlichen Bedenken bestehen**. Allerdings ist unbedingt die Zweckbindung und Datentrennung zu beachten, so dass die Zugriffsrechte des Call-Centers entsprechend einzuschränken sind (durch ein geeignetes Rollenkonzept), zumal die Einrichtung eines CRM-Systems der Vorabkontrolle bedarf, da Persönlichkeitsprofile mittels CRM-Systeme abgebildet werden können.
- Die Einhaltung der Auftragsvorgaben sollte daher im Rahmen der Auftragskontrolle (Nr. 6 in der Anlage zu § 9 BDSG) regelmäßig überprüft werden.

4.3 CRM-Zugriff d. ext. Call-Center (3)

Fallunterscheidung: (Fortsetzung)

2. Call-Center mittels Funktionsübertragung beauftragt:

- Bei einer Funktionsübertragung darf der Auftragnehmer eigene Interessen verfolgen. Folglich bedarf die Entscheidung über die Zulässigkeit einer Abwägung.
- Ein CRM-System bedarf bei der Einrichtung stets der Vorabkontrolle, da insbesondere Persönlichkeitsprofile von Kunden und Interessenten angelegt werden. Auch beim Betrieb ist daher sicherzustellen, dass keine besonderen Risiken für die Rechte und Freiheiten der Betroffenen durch den produktiven Betrieb entstehen. → Call-Center muss umfassende technische und organisatorische Maßnahmen vorweisen! → Zugriff auf CRM-System durch Call-Center (unter der Voraussetzung einer geeigneten Abschottung des CRM-Systems vor unbefugten Zugriffen) nur zulässig, wenn diesem keine Betroffeneninteressen entgegenstehen . Dies ist aus Aufgabenstellung nicht entscheidbar, allerdings bestehen hier **erhebliche Zweifel bei der Zulässigkeit**, da eine damit verbundene Zweckänderung fragwürdig bleibt.

4.4 Preisgabe von Daten & CRM-System

Aufgabe:

- Wenn ein Kunde nebenbei einem Call-Center-Agenten Informationen über sich preisgibt, dürfen diese in dessen CRM-System abgespeichert werden? Begründen Sie Ihre Antwort unter Nennung der entsprechenden Rechtsquellen! Gehen Sie bei Ihrer Antwort davon aus, dass das eingesetzte Call-Center Teil des Unternehmens ist, mit dem der Kunde ein Vertragsverhältnis unterhält.

4.4 Preisgabe von Daten & CRM-System (1)

- Ein Abspeichern personenbezogener Daten in einem CRM-System ist nach § 4 I BDSG nur zulässig, wenn eine Gesetzesvorschrift dieses erlaubt oder der Betroffene eingewilligt hat.
- Die Abspeicherung „nebenbei“ offenbarter Daten lässt sich nicht mit der Erfüllung des Geschäftszweckes und Vertragsverhältnisses nach § 28 I Nr. 1 BDSG begründen.
- „Nebenbei“ offenbarte Daten sind insbesondere auch nicht zwingend allgemein zugänglich im Sinne von § 28 I Nr. 3 BDSG.
- Da die „nebenbei“ erfolgte Preisgabe personenbezogener Daten weder zwingend auf der freien Entscheidung eines Betroffenen beruhen muss (Call-Center-Agenten weisen oftmals eine besondere Schulung ihrer Fragetechniken auf, um gerade die Preisgabe von Zusatzinformationen beim Plaudern zu erreichen!), noch der Kunde in allen Fällen davon ausgehen muss, dass entsprechende Äußerungen als Einwilligung im Sinne von § 4a I BDSG aufzufassen sind, ist diese Grundlage zumindest strittig. Selbst wenn dies als Gestattungserlaubnis anzusehen wäre, bedarf die Speicherung einer Einzelfallprüfung, ob diese noch verhältnismäßig ist, da z.B. auch ein Perspektivwechsel eintreten kann.

4.4 Preisgabe von Daten & CRM-System (2)

- Sofern die „nebenbei“ preisgegebenen Daten in einem direkten Verhältnis mit dem bestehenden Vertragsverhältnis oder vertragsähnlichen Vertrauensverhältnis steht, wird jedoch von einer Gestattung im Rahmen einer Einwilligung auszugehen sein.
- Sofern die „nebenbei“ preisgegebenen Daten im Rahmen üblicher Verhandlungsführungen anfallen, was z.B. bei Geschäftspartnern durchaus die Angabe, ob jemand gerne golfen geht, durchaus der Fall sein kann (sicherlich aber nicht bei Individualkunden), kann i.d.R. von einer Gestattung im Rahmen einer Einwilligung ausgegangen werden, dass beide Verhandlungsparteien über diese Geschäftspraktiken bescheid wissen (Besonderheit der B2B-Verhandlung).
- Bei B2C-Verhandlungen, also Gesprächen zwischen Anbieter und individuellen Endkunden kann hingegen nicht von einer Gestattung angegangen werden. Hier ist das schutzwürdige Interesse der Betroffenen höher zu gewichten! Dabei ist unerheblich, ob der Call-Center Teil des Unternehmens ist, mit dem das Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis besteht, oder ob der Call-Center sogar eigene Interessen vertritt. In keinem Fall wäre es aber zulässig im Rahmen einer Funktionsübertragung.

4.5 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 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!

4.5 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

4.5 Verfahren beim Kundendatenschutz (2)

Anmerkungen:

- Die Verfolgung des Herstellungsprozesses bestellter Güter mittels des ERP-Systems ist ggf. im Rahmen der Betriebsdatenerfassung 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 aufgrund innerbetrieblicher Aufgabenzuweisungen durch die Überwachung der RFID-Chips zugleich eine Mitarbeiterüberwachung (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 offenbart (Bewegung & Kaufverhalten)

4.5 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)

4.5 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. ggf. erfolgender Kreditkarteninformationseingabe!)
- Protokollierung der Datenübertragung (z.B. ans CRM-System) im Rahmen der Überwachung der Kundenhistorie

4.5 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