Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2016:

Kundendatenschutz (2)

3.1 Newsletter

Aufgabe:

- Ein Unternehmen möchte an seine Bestandskunden einen via E-Mail zu verschickenden Newsletter zustellen. Wie muss es hierzu vorgehen, um sowohl die datenschutzrechtlichen, telemedienrechtlichen und wettbewerbsrechtlichen Anforderungen zu erfüllen? Begründen Sie Ihre Antwort!

3.1 Newsletter (1)

Datenschutzrechtliche Anforderungen:

- Newsletter ist Instrument der Werbung
  → Vorgaben aus § 28 Abs. 3 & 4 BDSG zu beachten!
- Werbemaßnahmen erfordern nach § 28 Abs. 3 Satz 1 BDSG Einwilligung der Betroffenen, soweit nicht § 28 Abs. 3 Satz 2 einschlägig (aufgrund von: „Darüber hinaus“)
- Falls Einwilligungserklärung die Grundlage für den Newsletter-Versand darstellt, ist § 4a BDSG zu beachten!
- Bestandskunden = Listenmäßige bzw. sonst zusammengefasste Angehörige einer Personengruppe (nachweisbar anhand eines einzigen Kriteriums)
  → Ausnutzung des Listenprivilegs aus § 28 Abs. 3 Satz 2 Nr. 1 BDSG möglich
  → Dann ist Abwägung erforderlich (§ 28 Abs. 3 Satz 6 BDSG)

3.1 Newsletter (2)

Datenschutzrechtliche Anforderungen: Fortsetzung

- Newsletter darf nicht an Bestandskunden versandt werden, die diesem widersprochen haben (§ 28 Abs. 4 Satz 1 BDSG)
  → Prüfung, ob Widerspruch vorliegt
  → Eingesetztes System zu Planung und Versand von Newslettern muss Sperrfeld aufweisen, in das eingegangene Widersprüche eingetragen werden
- Angeschriebener Bestandskunde ist nach § 28 Abs. 4 Satz 2 BDSG bei jedem Newsletter zu benachrichtigen über
  ° die Identität der verantwortlichen Stelle und
  ° sein Widerspruchsrecht hinsichtlich dieser Werbeansprache
- Newsletter-Verfahren stellt ein eigenes Verfahren dar, das im Verfahrensverzeichnis aufzunehmen ist (Datum entsteht entweder durch Einwilligung oder via Listenprivileg zugunsten des Werbezwecks)

3.1 Newsletter (3)

Datenschutzrechtliche Anforderungen: Fortsetzung

- Alle Mitarbeiter, die mit dem Newsletter-Verfahren befasst sind, sind auf das Datengeheimnis nach § 5 BDSG zu verpflichten, da diese mit personenbezogene Daten umgehen
- Zum Schutz der Bestandskundendaten sind angemessene technische und organisatorische Maßnahmen zu ergreifen

3.1 Newsletter (4)

Telemedienrechtliche Anforderungen:

- Newsletter wird via E-Mail versandt
  → E-Mail ist telemedienrechtlicher Dienst
- Aufgrund von § 12 Abs. 1 TMG muss die Speicherung der Nutzerdaten für den Newsletter auf einer Rechtsvorschrift beruhen, die sich ausdrücklich auf Telemedien bezieht
  → Telemedienrecht ist ein Verweis auf das Listenprivileg nach § 28 Abs. 3 BDSG nicht rechtsbegründend
- Telemediendiensteanbieter darf personenbezogene Daten nur zu Zwecken verwenden, die telemedienrechtlich vorgeschrieben bzw. gestattet sind ODER zu denen die Nutzer eingewilligt haben (§ 12 Abs. 2 TMG)
  → Da TMG keine Gestattung zugunsten von Werbung kennt, ist das Vorliegen einer Einwilligungserklärung des Nutzer nötig!

3.1 Newsletter (5)

Telemedienrechtliche Anforderungen: Fortsetzung

- Für den Bezug eines Newsletters muss der Nutzer seine Einwilligung unter Beachtung von § 13 Abs. 3 TMG erteilen
  → Nutzer ist über sein Widerrufsrecht zu informieren!
- Einwilligungserklärung kann auch elektronisch erfolgen, wobei dann § 13 Abs. 2 TMG zu beachten ist:
  ° bewusste & eindeutige Erklärung des Nutzers
  ° Protokollierung der Einwilligungserklärung
  ° jederzeitige Abrufbarkeit der Einwilligungserklärung für Nutzer
  ° Umsetzung zum Widerrufsrecht
- Versand von Newslettern ist in der Datenschutzerklärung aufzuführen (§ 13 Abs. 1 TMG)
- Für den Abruf des Newsletters sind geeignete technische und organisatorische Maßnahmen zu ergreifen (§ 13 Abs. 4 TMG)

3.1 Newsletter (6)

Wettbewerbsrechtliche Anforderungen:

- Eine unzumutbare Belästigung durch eine Werbung via E-Mail liegt vor, wenn keine ausdrückliche Einwilligung des Empfängers vorliegt (§ 7 Abs. 2 Nr. 3 UWG) und/oder die Identität des Absenders verheimlicht oder verschleiert wird (§ 7 Abs. 2 Nr. 4 UWG)
- Keine unzumutbare Belästigung liegt jedoch nach § 7 Abs. 3 UWG) vor, wenn folgende Voraussetzungen gelten:
  ° Die E-Mail-Adresse wurde im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhoben (eine reine Interessenbekundung ist also nicht ausreichend!),
  ° Werbungen werden üblicherweise via E-Mail versandt,
  ° der Kunde hat der Werbung nicht widersprochen und
  ° der Kunde wird bei jeder Werbeansprache auf sein Widerspruchsrecht hingewiesen

3.2 Gewinnspiel & Werbung

Aufgabe:

- Ein Unternehmen möchte ein Gewinnspiel unter Beachtung von Wettbewerbsrecht und Datenschutzrecht durchführen, um über diesen Weg erreichen zu können, dass es volljährige Teilnehmer am Gewinnspiel (betrifft Bestandskunden als auch Interessenten) zu Werbezwecken kontaktieren darf. Ist es zulässig, dass die Teilnahme am Gewinnspiel an der Einwilligung zu Werbezwecken gekoppelt wird? Unterscheiden Sie bei Ihrer Antwort auch nach den Kontaktwegen Post, E-Mail und Telefon. Begründen Sie Ihre Antwort unter Angabe der Rechtsquellen!
  Hinweis:
  Zu vermeidende Vorgehensweisen bei Gewinnspielen sind in § 4 UWG und im Anhang zu § 3 Abs. 3 UWG beschrieben.
  Die Teilnahme am Gewinnspiel berechtigt dazu, an der Verlosung teilzunehmen, nicht aber garantiert einen Gewinn erzielen zu können. Insoweit resultiert aus der Teilnahme keine Leistungsverpflichtung im Sinne eines Vertrags.

3.2 Gewinnspiel & Werbung (1)

- Nach § 28 Abs. 3b BDSG besteht ein Kopplungsverbot darin, die Erbringung eines Vertrags davon abhängig zu machen, dass der Betroffene in die Verarbeitung oder Nutzung seiner Daten zu Werbezwecken einwilligt.
- Eine Teilnahme am Gewinnspiel begründet jedoch kein Vertragsverhältnis, da der Anbieter eines Gewinnspieles keinen Erfolg verspricht, sondern lediglich eine faire Chance auf einen Erfolg, indem der Teilnehmer an der Verlosung teilnimmt und dabei die gleiche Chance hat, gezogen zu werden, wie jeder andere Teilnehmer.
- Nach Voraussetzung der Aufgabe soll das Gewinnspiel unter Beachtung von Wettbewerbsrecht und Datenschutzrecht durchgeführt werden.
- Die Einwilligung in die Werbung soll dabei als Voraussetzung zur Teilnahme am Gewinnspiel gegeben werden.

3.2 Gewinnspiel & Werbung (2)

- Bei einer Einwilligung sind „lediglich“ die Voraussetzungen nach § 4a Abs. 1 BDSG zu erfüllen:
  - ° Freiwilligkeit gegeben, denn die Einwilligung in die Werbezwecke ist nicht an der Teilnahme beim Gewinnspiel gekoppelt, sondern anders herum.
  - ° Hinweis auf Zweck wird ausdrücklich gegeben (Werbezweck!), allerdings muss in der vorformulierten Einwilligungserklärung näher beschrieben werden, auf was genau sich die Werbung bezieht (z.B. durch präzisen Hinweis auf das bestehende Warensortiment bzw. den angebotenen Dienstleistungen; vgl. Beschluss des LG Berlin vom 09.08.2011; Az. 15 O 762/04).
  - ° Einwilligung zu Werbezwecken ist optisch hervorzuheben.
  - ° Einwilligung zu Werbezwecken darf jederzeit (also insbesondere nach Ablauf des Gewinnspiels) widerrufen werden.
  - ° Für Gewinnspiel wird eigene Einwilligung benötigt.

3.2 Gewinnspiel & Werbung (3)

- Laut Aufgabenstellung sollen sowohl Bestandskunden als auch Interessenten in die Werbung (und anschließend in das Gewinnspiel) einwilligen. Die Werbeerleichterung für Bestandskunden ist insoweit nicht fallrelevant.
- Datenschutzrechtlich ist insoweit die gewählte Konstruktion zulässig.
- Datenschutzrechtlich besteht kein Unterschied darin, ob die Einwilligenden anschließend per Post, E-Mail oder Telefon kontaktiert werden.
- Anders verhält sich das nach dem Wettbewerbsrecht. Doch ist erst mal zu klären, ob die gewählte Kopplung auch wettbewerbsrechtlich zulässig ist.
- Nach § 4 Nr. 5 UWG müssen die Teilnahmebedingungen des Gewinnspiels klar und eindeutig angegeben werden.
- Nach § 4 Nr. 6 UWG darf nicht der Erwerb einer Ware oder Dienstleistung von der Teilnahme am Gewinnspiel abhängig gemacht werden.

3.2 Gewinnspiel & Werbung (4)

- Gemäß Nr. 16 im Anhang zu § 3 Abs. 3 UWG wäre es unlauter, eine Erhöhung der Gewinnchance durch Bezug einer bestimmten Ware oder Dienstleistung zu versprechen.
- Nach Nr. 17 im Anhang zu § 3 Abs. 3 UWG wäre es zudem unlauter, den Eindruck zu erwecken, dass der Verbraucher einen Preis bereits gewinnen würde, wenn er eine bestimmte Handlung vornehmen würde (wie z.B. durch Einwilligung in Werbung).
- Nach Nr. 20 im Anhang zu § 3 Abs. 3 UWG wäre es schließlich unlauter, in Aussicht gestellte Preise nicht auch tatsächlich auszuschütten.
- Da laut Aufgabenstellung das Wettbewerbsrecht eingehalten werden soll, findet eine Verlosung unter den Teilnehmern statt, bei dem die Werbeeinwilligenden keinen garantierten Gewinn erhalten, sondern lediglich höhere Gewinnchancen, die aber in den Teilnahmebedingungen detailliert zu beschreiben wären (z.B. 2/3 vs. 1/3 je Lostopf).

3.2 Gewinnspiel & Werbung (5)

- Auch wettbewerbsrechtlich insoweit eine Kopplung der Teilnahme am Gewinnspiel an der Einwilligung in Werbung zulässig. Eine bloße Berücksichtigung der Werbeeinwilligenden ist aber unzulässig!
- Allerdings ist noch zu prüfen, welche Voraussetzungen an der Einwilligung in Werbung aus wettbewerbsrechtlicher Sicht bestehen:
  ° Werbung per Post nach § 7 Abs. 1 UWG nur dann unzumutbar, wenn die Werbung z.B. aufgrund eines Widerspruchs (im Sinne von § 28 Abs. 4 BDSG) offensichtlich unerwünscht ist
  ° Werbung per Mail dagegen darüber hinaus für Interessenten nur zulässig, wenn der Verbraucher in die Werbung (und die Ansprache per Mail) eingewilligt hat (§ 7 Abs. 2 Nr. 3 UWG), z.B. durch freiwillige Angabe der Mail-Adresse; Bestandskunden dürfen angemailt werden, wenn § 7 Abs. 3 UWG berücksichtigt wurde
  ° Werbung per Telefon dagegen nur zulässig, wenn der Verbraucher ausdrücklich darin eingewilligt hat (§ 7 Abs. 2 Nr. 2 UWG)

3.3 Datenschutzerklärung

Aufgabe:

- Ein Reisevermittlungsanbieter bietet Nutzern ihres Web-Portals die Möglichkeit, Reiseleistungen bei entsprechenden Anbietern online zu buchen. Hierzu tragen die Nutzer geforderte personenbezogene Reisedaten in das bereitgestellte Web-Formular ein. Diese Daten werden anschließend an den jeweiligen Reiseanbieter übermittelt. Formulieren Sie eine erläuternde Datenschutzerklärung gemäß den Anforderungen aus § 13 Abs. 1 TMG, die auf der betreffenden Web-Seite abrufbar sein soll!
- *Hinweis:*
  Zweck der Datenerhebung und –speicherung ist folglich die geschäftsmäßige Übermittlung an die Reiseanbieter.

3.3 Datenschutzerklärung (1)

- Bei jedem Zugriff auf unsere Homepage wird zu systembezogenen statistischen Zwecken und zur Gewährleistung unseres Web-Angebotes protokolliert:
  - Bezeichnung der aufgerufenen Web-Site
  - Datum und Uhrzeit des Zugriffs
  - Umfang des übertragenen Datenvolumens
  - Systemmeldung zum Erfolg des Aufrufs
  - Angaben zum eingesetzten Webbrowser
  - IP-Adresse des aufrufenden Rechners
  - Webadresse, von der aus auf das Web-Angebot zugegriffen wurde
- Diese Protokolldaten werden nach sechs Monaten gelöscht.

3.3 Datenschutzerklärung (2)

- Weitergehende personenbezogene Daten werden lediglich erhoben, wenn der Nutzer diese Angaben beim Ausfüllen des Web-Formulars angibt. Zur Vermittlung von Online-Buchungen von Reiseleistungen bei entsprechenden Anbietern werden dazu benötigt:
  - Name des Nutzers
  - Reisedaten des Nutzers (Reisezeitraum, Ort, ggf. zu buchende Verkehrsmittel)
  - Kontaktdaten des Nutzers (für Rückfragen bzw. Umbuchungsmitteilungen)

  In den vorliegenden Freitextfeldern können vom Nutzer weitere personenbezogene Daten freiwillig angegeben werden.
- Alle angegebenen personenbezogenen Daten werden ausschließlich zur Übermittlung an die Reiseanbieter verwendet und unterliegen den gesetzlichen Datenschutzbestimmungen.

3.3 Datenschutzerklärung (3)

- Die an die Reiseanbieter zu übermittelnden Daten werden zwei Monate lang gespeichert, um etwaige Rückfragen des Reiseanbieters beantworten zu können und sicherstellen zu können, dass die gewünschte Online-Buchung den Reiseanbieter auch tatsächlich erreicht hat.
- Sie haben jederzeit das Recht auf Auskunft über die bezüglich Ihrer Person bei uns gespeicherten Daten, deren Herkunft und die Angabe etwaiger Empfänger sowie den Zweck der Speicherung. Auskunft erteilt Ihnen hierzu unser Datenschutzbeauftragte [Link].
- Inhalte und Funktionalitäten unserer Web-Seiten werden unter größtmöglicher Sorgfalt implementiert und regelmäßig aktualisiert. Dennoch können wir etwaige Störungen unseres Web-Angebots nicht ausschließen. Für externe Links auf Angaben der Reiseanbieter können wir keine Haftung übernehmen.

3.3 Datenschutzerklärung (4)

- Angaben zur Stelle des Reisevermittlungsdienstes [bzw. Link zum Impressum] und zu den Reisedienstleistern, deren Angebote verlinkt wurden

Hinweis:

- Würden auch Cookies eingesetzt, wäre neben § 13 Abs. 1 Satz 1 TMG auch Satz 2 zu berücksichtigen, da Cookies als automatisiertes Verfahren anzusehen sind.

3.4 Auftragsdatenverarbeitung Call-Center

Aufgabe:

- Ein Call-Center wertet für seine Auftraggeber Daten in deren CRM-System aus, reichert die Daten über die Betroffenen (Endverbraucher) um öffentlich verfügbare Informationen an und führt Kundenzufriedenheitsbefragungen durch. Was muss der Auftraggeber wie regeln, damit die Tätigkeit des Call-Centers nicht als Funktionsübertragung anzusehen ist? Geben Sie hierzu die zugehörigen Rechtsquellen an!

3.4 Auftragsdatenverarbeitung Call-Center (1)

Call-Center-Tätigkeit nur dann Auftragsdatenverarbeitung, wenn Voraussetzungen aus § 11 BDSG voll erfüllt sind:

→ Schriftliche Vereinbarung nötig (§ 11 II BDSG)
→ darin Beschreibung des 10-Punkte-Katalogs aus § 11 II BDSG (vollständig, da sonst Bußgeldtatbestand)
→ Auftraggeber muss sich vor Beginn der Tätigkeit des Call-Centers davon überzeugen, dass Call-Center angemessene technische und organisatorische Maßnahmen zum Schutz der Daten des Auftraggebers getroffen hat (§ 11 II BDSG)
→ Call-Center hat getroffene Schutzmaßnahmen nach § 9 BDSG zu beschreiben und Auftraggeber vorzulegen
→ Maßnahmenprüfung ist zu dokumentieren (§ 11 II BDSG)

3.4 Auftragsdatenverarbeitung Call-Center (2)

→ Auftraggeber muss sicherstellen, dass Call-Center-Tätigkeit zulässig ist (§ 11 I BDSG)

→ Detaillierte Festlegung, welche öffentlich verfügbaren Daten durch Call-Center hinzugefügt werden sollen (Derartiges hinzufügen ist keine klassische Tätigkeit eines Call-Centers!)

→ Kundenzufriedenheitsbefragungen dagegen Kerntätigkeit eines Call-Centers

→ Auftraggeber muss sich Weisungsrecht vorbehalten (§ 11 III BDSG)

→ Call-Center hat ausführende Agenten auf das Datengeheimnis nach § 5 BDSG zu verpflichten (§ 11 IV BDSG)

3.5 Schutzmaßnahmen

Aufgabe:

- Ein Unternehmen betreibt hinsichtlich des Umgangs mit Kundendaten folgende technischen Systeme: Web-Portal zur Erhebung von Bestellwünschen, ERP-System zur 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 technischen und organisatorischen Maßnahmen sind für die Verfahren im Rahmen der Kundendatenverwaltung zwingend, damit keine besonderen Risiken für die Rechte und Freiheiten der Betroffenen davon ausgehen können? Begründen Sie Ihre Antwort!

3.5 Schutzmaßnahmen (1)

Schutz des Web-Portals (= Kundengewinnungsverfahren):

- Zuverlässiges Authentifizierungsverfahren
  → Gewährleistung, dass Kunde eindeutig bestimmt wird
- Opt-in-Lösung für Bestellungen zur Kontrolle für Betroffenen
  → Abwicklung über Web-Portal erfordert technische Absicherung
- Manipulationsschutz für Eintragungen mittels Datenvalidierung & Vergabe restriktiver Schreibrechte
  → Vermeidung von Systemkompromittierungen bzw. DoS-Attacken
- Keine Upload-Funktion, um Malware-Einspeisung zu verhindern
  → Verhinderung einer Ausspähung durch Trojanische Pferde

3.5 Schutzmaßnahmen (2)

Schutz des Web-Portals (= Kundengewinnungsverfahren): Forts.

- Redundante Technik zur Ausfallsicherheit des Web-Portals
  → Nichterreichbarkeit des Web-Portals führt sonst ggf. zu Umsatzausfall
- Protokollierung der Datenübertragung (z.B. ans ERP-System) im Rahmen der Bestellabwicklung
  → Telemedienrechtlicher Nachweis, dass Bestellung tatsächlich erteilt wurde
- Vermeidung einer unmittelbaren Übertragung der Bestellung vom Web-Portal ins LAN (Holsystem statt Bringsystem)
  → Kein Durchgriff vom Internet ins LAN im Rahmen der Netzwerksegmentierung und -segregation

3.5 Schutzmaßnahmen (3)

Schutz des Buchhaltungssystems (= Kundenbetreuungsverfahren):

- Wirksamer Zugriffsschutz
  → Gewährleistung, dass auf Buchhaltungsdaten nur zugreifen darf, der gemäß seiner betrieblichen Aufgaben auch begründet darauf zugreifen können muss
- Einsatz eines geeigneten Benutzerrollenkonzepts, da ERP-System auch andere Funktionen erfüllt
  → Wirksame Beschränkung von Zugriffsrechten unter Berücksichtigung der innerbetrieblichen Organisation
- Protokollierung von Eingaben, Veränderungen & Löschungen, um kompletten Prozess nachweisen zu können
  → Nachweis der Eingabekontrolle

3.5 Schutzmaßnahmen (4)

Schutz des Buchhaltungssystems (= Kundenbetreuungsverfahren):

- Besonderes Augenmerk auf ggf. bestehende Schnittstellen zur Kontenverwaltung (Online-Banking bzw. eCash-Verwaltung, sofern vorgesehen – dann ergänzende Anforderungen bei Web-Portal wg. Bank-/Kreditkartendateneingabe!)
  → Vermeidung einer meldepflichtigen Datenpanne
- Protokollierung der Datenübertragung (z.B. ans CRM-System) im Rahmen der Überwachung der Kundenhistorie
  → Umsetzung der Weitergabekontrolle

3.5 Schutzmaßnahmen (5)

Schutz des CRM-Systems (= Kundenbindungsverfahren):

- Gewährleistung der Zweckbindung
  → Umsetzung des Trennungsgebots
- Wirksamer Zugriffsschutz (i.d.R. andere Zugriffsberechtigte als beim Buchführungssystem wg. Segregation of Duties!)
  → Umsetzung der Zugriffskontrolle
- Bereitstellung von anonymisierten Reports (→ Vermeidung von Drill-Down-Funktionen)
  → Grundsatz der Datensparsamkeit
- Regelmäßige Kontrollen, ob eine unzulässige Datenanreicherung stattfand
  → Vermeidung einer ungewollten Erhöhung des Schutzbedarfs

3.5 Schutzmaßnahmen (6)

Schutz des CRM-Systems (= Kundenbindungsverfahren):

- Protokollierung über Anfertigung spezifischer Auswertungen & Beschränkung möglicher Auswertungsfunktionen
  → Nachweis zur Weitergabekontrolle
  → Prävention unzulässiger Datenverwendungen
- Sperrfeld zur Berücksichtigung von Werbewidersprüchen
  → Umsetzung sowohl datenschutzrechtlicher als auch wettbewerbsrechtlicher Verstöße durch Nichtbeachtung des jeweiligen Widerspruchsrechts