# Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2012:
Kundendatenschutz (2) & Mediendatenschutz

# 3.1 Elektronische Einwilligung

**Aufgabe**:

- Formulieren Sie eine elektronische Einwilligungs-erklärung, die die Anforderungen aus dem TMG erfüllt, anhand eines frei gewählten Beispiels!

# 3.1 Elektronische Einwilligung

Hiermit willige ich ein, dass die im voranstehenden Web-Formular angegebenen personenbezogenen Daten von der <Bezeichnung der verantwortlichen Stelle> zum Zweck der <Zweck> erhoben, verarbeitet und genutzt werden dürfen. Ich wurde darüber informiert, dass ich diese Einwilligung jederzeit ohne Nachteile widerrufen kann und meine Angaben jederzeit unter <Link> abrufen kann. Mir ist bewusst, dass aus Gründen der Nachvollziehbarkeit der Vorgang der Einwilligung selbst mitprotokolliert wird. Von der <Bezeichnung der verantwortlichen Stelle> wurde mir versichert, dass meine datenschutzrechtlichen Belange ohne Einschränkung gewährleistet werden und keine Übermittlung meiner Daten an Dritte erfolgt.

☐ Obiger Einwilligungserklärung stimme ich zu! *(bitte Häkchen setzen)*

☒ *Absenden!*

# 3.2 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 TMG, die auf der betreffenden Web-Seite abrufbar sein soll!
- *Hinweis:*
  *Zweck der Datenerhebung und –speicherung ist folglich die geschäftsmäßige Übermittlung an die Reiseanbieter.*

# 3.2 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.

# 3.2 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.

# 3.2 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.

# 3.2 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.

# 3.3 Web-Tracking

**Aufgabe**:

- Ein Unternehmen möchte die Nutzung ihrer Webseite mittels eines Tracking-Tools analysieren, das die IP-Adressen der Nutzer und die getätigten Klicks sowie die eingegebenen Suchanfragen zu Analysezwecken an einen für derartige Analysen spezialisierten Dritten überträgt. Das Unternehmen in den USA, das diese Analysen vornehmen soll, behält sich die Verwendung der empfangenen Daten für eigene Zwecke vor. Ist die Verwendung eines derartigen Tracking-Tools zulässig? Begründen Sie Ihre Antwort unter Angabe der Rechtsquellen!
- *Hinweis:*
  *Ziel von Tracking Tools im telemedienrechtlichen Sinn ist die bedarfsgerechte Gestaltung angebotener Telemedien.*

# 3.3 Web-Tracking (1)

Hinweise:

- IP-Adressen werden nach herrschender Meinung als personenbezogene Daten angesehen (siehe auch das Beispiel 15 zu dynamischen IP-Adressen in WP 136 der EU-Datenschutzgruppe nach Art. 29 EU-DSRL)
- Aufgabe von Tracking-Tools ist es, das Verhalten der Web-Seiten-Nutzer hinsichtlich deren Klicks und Eingaben auf den bereitgestellten Web-Seiten zu analysieren und daraus Rückschlüsse zur Verbesserung des eigenen Web-Auftritts bzw. der dort angebotenen Produkte/Leistungen ziehen zu können
  → Ziel: bedarfsgerechte Gestaltung angebotener Telemedien!
  → Zulässigkeit des Einsatzes von Tracking-Tools prüfen und
  → Zulässigkeit der Übermittlung der Daten prüfen!

# 3.3 Web-Tracking (2)

- Nach § 15 III TMG darf ein Dienstanbieter zum Zweck der […] bedarfsgerechten Gestaltung der angebotenen Telemedien Nutzungsprofile unter Verwendung von Pseudonymen (!) erstellen, sofern der Nutzer diesem nicht widerspricht.
  → Auf den Einsatz des Tools und 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.
- Ist für den vorgesehenen Zweck der Auswertung kein Personenbezug erforderlich (z.B. bei rein statistischen Analysen), ist bei der Auswertung auf die IP-Adressen-Speicherung im Sinne der Datensparsamkeit und § 13 VI TMG zu verzichten
  → Dann keine Restriktionen zu beachten (Erhebung zulässig!)

# 3.3 Web-Tracking (3)

- Für den Fall einer zulässigen Verwendung hat der Einsatz des Web-Tracking-Tools stets unter Einsatz ausreichender technischer und organisatorischer Maßnahmen zu erfolgen nach § 13 IV TMG bzw. § 9 BDSG, da IP-Adressen und zu trackende Nutzereingaben ggf. Personenbezug aufweisen (siehe auch Hinweis!).
- An dieser Stelle laut Aufgabenstellung noch kein Entscheidungskriterium über Zulässigkeit möglich
  → Fallunterscheidung:
    1. Übermittelte Daten mit Personenbezug? (davon ist gemäß obigem Hinweis auszugehen!)
    2. Übermittlung an sich zulässig?

# 3.3 Web-Tracking (4)

Fallunterscheidung: Gegebener Personenbezug der Daten:

- Sofern die IP-Adressen und ggf. weitere personenbezogene Daten (Such-Anfragen, Einträge in Web-Formulare etc.) mittels des Web-Tracking-Tools analysiert werden sollen, ist aufgrund der damit verbundenen Zweckänderung (!) die **Einwilligung der Betroffenen erforderlich** nach § 12 II TMG!
  → **Liegt keine derartige Einwilligungserklärung vor, ist die Verwendung des Tracking-Tools (und erst recht die Datenübermittlung ins Ausland) unzulässig!** (in Aufgabenstellung zum Vorliegen einer derartigen Einwilligungserklärung aber keine Hinweise vorhanden → Unzulässigkeit wahrscheinlich)

# 3.3 Web-Tracking (5)

Fallunterscheidung zur Übermittlung (1):

- **Übermittlung** personenbezogener Daten **nur zulässig**, **wenn**
  a) **Datensender** dazu **befugt** (möglich nach § 28 II Nr. 1 BDSG i.V.m. § 28 I Nr. 2 BDSG) und
  b) **bei Datenempfänger** ein **angemessendes Datenschutzniveau** gilt, wenn die Daten ins Ausland transferiert werden sollen (§ 4b II BDSG)
  → Überprüfung, ob Betroffener ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat (aus Aufgabenstellung nicht unmittelbar ersichtlich)
  → Klärung, ob bei Empfängerstelle ein angemessenes Datenschutzniveau im Sinne von § 4b III BDSG besteht (*in USA bei Unternehmen im Safe Harbor Programm ggf. gegeben*)

# 3.3 Web-Tracking (6)

Fallunterscheidung zur Übermittlung (2):

- Nach Aufgabenstellung jedoch keine Angabe, ob bei Datenempfänger ein ausreichendes Datenschutzniveau vorhanden ist
  → Starkes Indiz für Unzulässigkeit
- Nach Aufgabenstellung verfolgt der Datenempfänger eigene Zwecke mit den empfangenen und zu analysierenden Daten
  → Zweckbestimmung aus § 4b III BDSG nicht durchgreifend
  → keine Zweckbindung nach § 4b VI BDSG gegeben
  → Betroffeneninteresse am Ausschluss stärker zu gewichten!
  → anhand vorhandener Aufgabendaten nicht genügend „Gegengewicht“ bei Abwägung vorhanden
  → **Übermittlung in die USA als unzulässig anzusehen**!

# 3.4 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!

# 3.4 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)

# 3.4 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)

# 3.4 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

# 3.4 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!

# 3.4 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)

# 3.4 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

# 3.5 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