Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2011:
Mediendatenschutz & Kundendatenschutz (3)

3.1 Elektronische Einwilligung

Aufgabe:

- Formulieren Sie eine elektronische Einwilligungserklärung, 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 Unternehmen möchte ihren Nutzern im Internet die Möglichkeit einräumen, Anfragen zu den auf eigenen Web-Seiten dargestellten Dienstleistungen durch Ausfüllen eines Web-Formulars stellen zu können. Dabei werden auch personenbezogene Daten erhoben und übertragen. Formulieren Sie eine erläuternde Datenschutzerklärung gemäß den Anforderungen aus § 13 TMG, die auf der betreffenden Web-Seite abrufbar sein soll!

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
- Die gespeicherten Protokolldaten werden nach 6 Monaten gelöscht.

3.2 Datenschutzerklärung (2)

- Weitergehende personenbezogene Daten werden lediglich erhoben, wenn der Nutzer diese Angaben beim Ausfüllen des Web-Formulars freiwillig angibt. Für die Bearbeitung etwaiger Anfragen zu unseren Dienstleistungen werden dazu benötigt:
  - Name des Nutzers
  - Mail-Adresse, an die unsere Antworten gesandt werden sollen

  In den vorliegenden Freitextfeldern können vom Nutzer weitere personenbezogene Daten freiwillig angegeben werden.
- Die Einwilligung kann jederzeit mithilfe des Web-Formulars abgerufen bzw. widerrufen werden.
- Alle angegebenen personenbezogenen Daten werden ausschließlich für die Beantwortung der Anfragen verwendet und unterliegen den gesetzlichen Datenschutzbestimmungen.

3.2 Datenschutzerklärung (3)

- Enthalten die gemachten Angaben Bestelldaten oder Daten zur Vertragsabwicklung, werden diese Angaben an den Vertrieb weitergeleitet.
- 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 fremde Inhalte können wir keine Haftung übernehmen.

3.2 Datenschutzerklärung (4)

- Angaben zur verantwortlichen Stelle [bzw. Link zum Impressum]

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 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!

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 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!

3.4 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)
  [außerdem: Anruf durch Call-Center = Nutzung von Telekommunikation
  → Fernmeldegeheimnis (§ 88 TKG) zu beachten
  → Call-Center hat angemessene Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten zu treffen (§ 109 I Nr. 1 TKG)]

3.4 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 (Voraussetzung für Auftragserteilung!).
- 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 ist im Rahmen der Auftragskontrolle (§ 11 II BDSG i.V.m. Nr. 6 in der Anlage zu § 9 BDSG) **regelmäßig zu überprüfen**.

3.4 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 (§ 28 II Nr. 1 BDSG i.V.m. § 28 I Nr. 2 BDSG).
- 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.

3.5 Datenschutzrisiko gemäß Vorabkontrolle

Aufgabe:

- Für ein geplantes Kundenbetreuungsverfahren (alle Kunden sind Endverbraucher) mittels Web-Portal wurden seitens des Vertriebs folgende Anforderungen formuliert:
  - Das Web-Portal soll auf die Kundendaten des CRM-Systems automatisiert zugreifen können (sowohl lesend als auch schreibend)
  - Die Kunden sollen eine fortlaufende Nummer als Benutzerkennung erhalten und das Web-Portal nach Eingabe eines frei gewählten Passwortes nutzen können
  - Für durchgeführte Bestellungen sollen die Kunden eine Bestätigungsmail erhalten
  - Im Web-Portal sollen die Kunden ihre Bestellhistorie einsehen können

  Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer Vorabkontrolle sehen, schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß angefügter 5x5-Risk Map. Sofern Handlungsbedarf besteht, geben Sie eine passende Maßnahme an.

3.5 Datenschutzrisiko gemäß Vorabkontrolle (1)

A) Ermittlung potenzieller Datenschutzrisiken:

- Lesender & schreibender Zugriff des Web-Portals auf CRM-System
  1. Unbeschränkter Zugriff auf alle CRM-Daten
  2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben
- Benutzerkennung via fortlaufender Nummer & freie Passwortwahl
  3. Enumerative Zugangsdaten
  4. Mangelnder Zugriffsschutz bei geringer Passwortgüte
- Bestätigungsmail für durchgeführte Bestellungen
  5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
- Einsicht in Bestellhistorie via Web-Portal
  6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil

Bei 1., 2., 5. und 6. unmittelbarer Zugriff auf personenbezogenen Daten

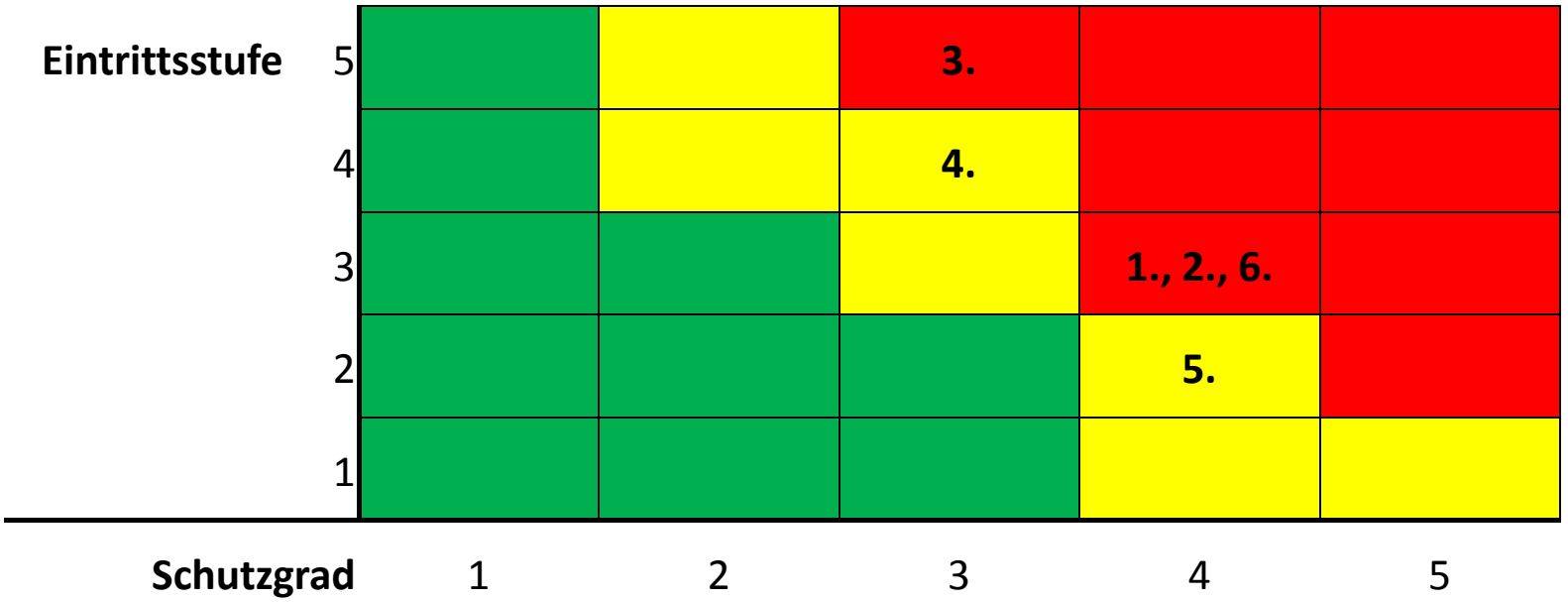
→ Schutzgrad 4; bei 3. und 4. dagegen Schutzgrad 3 (Pseudonym)

3.5 Datenschutzrisiko gemäß Vorabkontrolle (2)

B) Abschätzung der Eintriffsstufe:

1. Unbeschränkter Zugriff auf alle CRM-Daten: 3, da Angreifer über begrenzte Fähigkeiten & Ressourcen verfügen muss, um Daten z.B. via SQL-Injection abrufen zu können
2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben: 3, da ebenfalls via SQL-Injection
3. Enumerative Zugangsdaten: 5, da Ausprobieren voraussetzungslos
4. Mangelnder Zugriffsschutz bei geringer Passwortgüte: 4, da Passwort-Cracker leicht downloadbar sind & schlechte Passwörter i.d.R. bereits leicht zum Erfolg führen (z.B. Benutzerkennung = Passwort)
5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden: 2, da Verbindungspfad erst ermittelt werden muss
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil: 4, wg. 3. & 4.

3.5 Datenschutzrisiko gemäß Vorabkontrolle (3)



Rot = Aktivität nötig; **Gelb** = Aktivität prüfen; **Grün** = Akzeptabel

3.5 Datenschutzrisiko gemäß Vorabkontrolle (4)

C) Handlungsempfehlung:

1. Unbeschränkter Zugriff auf alle CRM-Daten
   → Datenvalidierung sicherstellen
2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben
   → Schreibenden Zugriff auf CRM unterbinden
3. Enumerative Zugangsdaten
   → Benutzerkennung frei wählen lassen
4. Mangelnder Zugriffsschutz bei geringer Passwortgüte
   → Mindestvorgaben für Passwortgüte festlegen
5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
   → ggf. akzeptierbar
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil
   → nach Änderung zu 3. & 4. ggf. akzeptierbar