

Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2010:
TMG & Kundendatenschutz (2)

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 sollenIn 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 u.U. erwartbar*)

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 Webseiten 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 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 Lagerverwaltungssystem 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!

3.5 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

3.5 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)*

3.5 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)

3.5 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. erfolgreicher Kreditkarteninformationseingabe!)
- Protokollierung der Datenübertragung (z.B. ans CRM-System) im Rahmen der Überwachung der Kundenhistorie

3.5 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