Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2013:

Kundendatenschutz (1)

2.1 Verfahrensverzeichnis

Aufgabe:

- Erstellen Sie anhand der Auflistung aus § 4e BDSG das vom Datenschutzbeauftragten zu veröffentlichende "Verfahrensverzeichnis" für nachfolgend benannte Verfahren zum Kundendatenschutz eines Web-Shops! Gehen Sie bei Ihrer Lösung davon aus, dass der Web-Shop folgende Web-Formulare bereithält und nur zugehörige Verfahren im Kontext der Kundendatenverarbeitung durchführt:
  ° Aufnahme der Bestellung
  ° Bezug und Abbestellung des Newsletters
  ° Kontaktmöglichkeit für Rückfragen
  Auf den Web-Seiten selbst sind keine kundenspezifische Daten abrufbar. Der Web-Shop richtet sich ausschließlich an Endverbraucher.

2.1 Verfahrensverzeichnis für Kundendatenverwaltung (1)

- **Öffentliches Verfahrensverzeichnis** = Auflistung der Punkte 1 – 8 aus § 4e BDSG (nach § 4g Abs. 2 BDSG)
- Web-Shop → Geschäftszweck: Online-Verkauf von Gütern
- Web-Formular zur Aufnahme der Bestellung
  → Bestellung, Güterversand, Rechnungswesen, Finanzbuchhaltung
  → rechtsgeschäftliches Schuldverhältnis (= Kaufvertrag!)
  → Betroffene: Kunden
  → Datenverwendungszweck: **Vertragserfüllung Online-Verkauf**
  → Datenkategorien: Identifikationsdaten, Versanddaten (Zustelladressdaten), ggf. Kontaktdaten, Bestelldaten, Rechnungsdaten, Zahlungsdaten

2.1 Verfahrensverzeichnis für Kundendatenverwaltung (2)

- Web-Formular zu Bezug & Abbestellung des Newsletters
  → Newsletterversand
  → rechtsgeschäftsähnliches Schuldverhältnis (= Werbung!)
  → Betroffene: Kunden oder Interessenten
  → Datenverwendungszweck: **Newsletterabwicklung**
  → Datenkategorien: Identifikationsdaten, Maildaten, Daten über Bezug & Abbestellung des Newsletters

2.1 Verfahrensverzeichnis für Kundendatenverwaltung (3)

- Web-Formular zur Kontaktmöglichkeit für Rückfragen
  → Kundenbetreuung
  → Anfragen von Interessenten = rechtsgeschäftsähnliches Schuldverhältnis
  → Rückfragen von Kunden = rechtsgeschäftliches Schuldverhältnis
  → Betroffene: Kunden oder Interessenten
  → Datenverwendungszweck: **Anfragebearbeitung**
  → Datenkategorien: Identifikationsdaten, Kontaktdaten (für Antworten), Anfragedaten, Antwortdaten

2.1 Verfahrensverzeichnis für Kundendatenverwaltung (4)

1. Name oder Firma der verantwortlichen Stelle:
   Web-Shop P.U.R. GmbH & Co. KG
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen:
   Geschäftsführer: Peter Müller
   Vertriebsleiter: Josef Schmidt
   EDV-Leiterin: Andrea Schulze
3. Anschrift der verantwortlichen Stelle:
   Web-Shop P.U.R. GmbH & Co. KG
   Musterstr. 1
   12345 Musterstadt

2.1 Verfahrensverzeichnis für Kundendatenverwaltung (5)

4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung:
   A) Vertragserfüllung Online-Verkauf
   B) Newsletter
   C) Anfragebearbeitung
5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien:
   Betroffene A): Kunden
   Betroffene B) und C): Kunden & Interessenten
   Datenkategorien A): Identifikationsdaten, Versanddaten, ggf. Kontaktdaten, Bestelldaten, Rechnungsdaten, Zahlungsdaten
   Datenkategorien B): Identifikationsdaten, Maildaten, Daten über Bezug & Abbestellung des Newsletters
   Datenkategorien C): Identifikationsdaten, Kontaktdaten, Anfragedaten, Antwortdaten

2.1 Verfahrensverzeichnis für Kundendatenverwaltung (6)

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:
   A): Inkassounternehmen bei Zahlungsverzug, öffentliche Stellen aufgrund gesetzlicher Vorgaben, interne Stellen (Finanzbuch-haltung) zur Aufgabenerfüllung
   B): entfällt
   C): interne Stellen, soweit von Anfrage betroffen
7. Regelfristen für die Löschung der Daten:
   A), B) und C): 6 Jahre (Geschäftsbriefe),
   A): 10 Jahre (Buchungsdaten)
8. eine geplante Datenübermittlung in Drittstaaten:
   A), B) und C): entfällt

2.2 Datenschutzrisiko gemäß Vorabkontrolle

Aufgabe:

- Für ein geplantes Kundenbetreuungsverfahren (alle Kunden sind Endverbraucher) mittels Web-Portal wurden seitens des Vertriebs folgende Wünsche 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 (gem. § 4d Abs. 5 BDSG) sehen, schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß nachstehender 3x3-Risk-Map. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

2.2 Datenschutzrisiko gemäß Vorabkontrolle (1)

A) Ermittlung potenzieller Datenschutzrisiken:

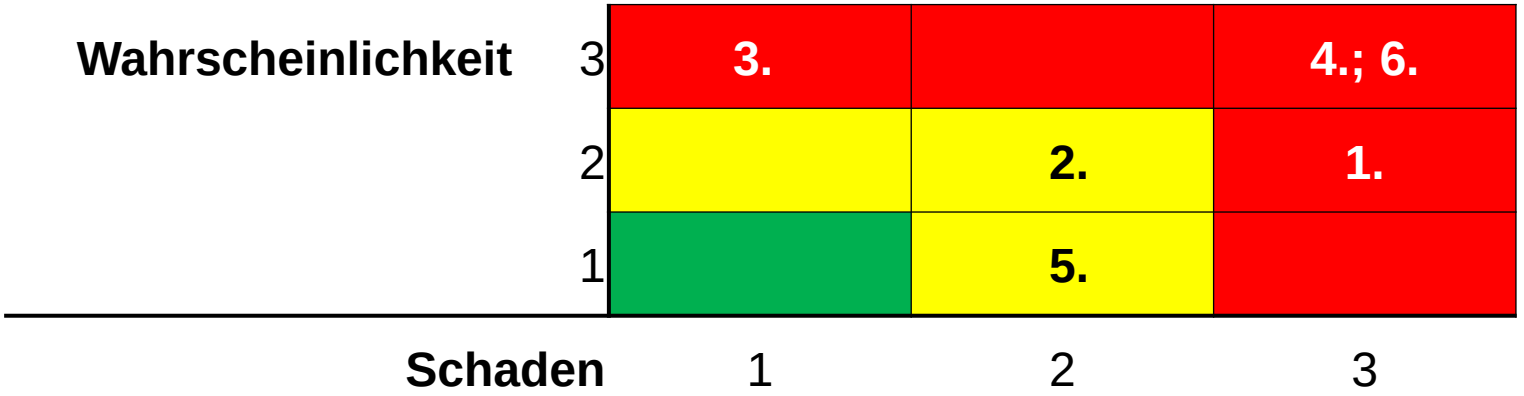
- Lesender & schreibender Zugriff des Web-Portals auf CRM-System
  1. Unbeschränkter Zugriff auf alle CRM-Daten → Gefahr: Unbefugte Datenbereithaltung zum Abruf (§ 43 Abs. 2 Nr. 2 BDSG)
  2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben → Gefahr: Formaler Verstoß gegen Eingabekontrolle (Anlage zu § 9 BDSG)
- Benutzerkennung via fortlaufender Nummer & freie Passwortwahl
  3. Enumerative Zugangsdaten → Gefahr: kein unmittelbarer Schaden
  4. Mangelnder Zugriffsschutz bei geringer Passwortgüte → Gefahr: Unbefugte Datenbereithaltung zum Abruf (§ 43 Abs. 2 Nr. 2 BDSG)
- Bestätigungsmail für durchgeführte Bestellungen
  5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden → Gefahr: Formaler Verstoß gegen Weitergabekontrolle (Anlage zu § 9 BDSG)
- Einsicht in Bestellhistorie via Web-Portal
  6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil → Gefahr: Unbefugte Datenbereithaltung zum Abruf (§ 43 Abs. 2 Nr. 2 BDSG)

2.2 Datenschutzrisiko gemäß Vorabkontrolle (2)

B) Abschätzung der Eintriffsstufe:

1. Unbeschränkter Zugriff auf alle CRM-Daten: Gefahreintritt wahrscheinlich, da Angreifer nur über begrenzte Fähigkeiten & Ressourcen verfügen muss, um Daten z.B. via SQL-Injection abrufen zu können
2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben: Gefahreintritt wahrscheinlich, da ebenfalls via SQL-Injection ausnutzbar
3. Enumerative Zugangsdaten: Gefahreintritt sicher, da entsprechendes Auspro-bieren voraussetzungslos möglich ist
4. Mangelnder Zugriffsschutz bei geringer Passwortgüte: Gefahreintritt sicher, 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: Gefahreintritt möglich, da Angreifer erst noch den Verbindungspfad ermitteln muss
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil: Gefahreintritt sicher, aufgrund der Voraussetzungen aus 3. & 4.

2.2 Datenschutzrisiko gemäß Vorabkontrolle (3)



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

Wahrscheinlichkeit: **Eintritt einer Verletzung des informationellen Selbstbestimmungsrechts**	**Schaden:** **Grad der Verletzung des informationellen Selbstbestimmungsrechts**
1 = möglich	1 = niedrig (ohne unmittelbare Wirkung)
2 = wahrscheinlich	2 = mittel (formaler Verstoß)
3 = sicher	3 = hoch (Bußgeld/Datenpanne)

2.2 Datenschutzrisiko gemäß Vorabkontrolle (4)

C) Handlungsempfehlung:

1. Unbeschränkter Zugriff auf alle CRM-Daten
   → Datenvalidierung sicherstellen (SQL-Injection verhindert)
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 (Komplexität, Länge)
5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
   → ggf. akzeptierbar, wenn Verbindungspfad nicht ermittelbar ist
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil
   → nach Änderung zu 3. & 4. ggf. akzeptierbar

2.3 Kundenspezifische Datenanalysen

Aufgabe:

- Ein Unternehmen möchte ein datenschutzkonformes Customer-Relationship-Management-System (CRM-System) einführen. In diesem CRM-System sollen alle kundenspezifische Daten zusammengetragen werden, die das Unternehmen bereits in verschiedenen Quellen gespeichert hat. Zu den Kunden zählen ausschließlich Privatpersonen. **Wie muss das Unternehmen hierzu vorgehen?** Begründen Sie Ihre Antwort!

2.3 Kundenspezifische Datenanalysen (1)

- Unternehmen = nicht-öffentliche Stelle
- CRM-System = System zur Kunden**bewertung**
  → Vorabkontrolle erforderlich (§ 4d V BDSG)
  → Vorabkontrolle durch DSB (§ 4d VI BDSG)
  → DSB muss bestellt sein / werden (§ 4f I BDSG)
- Hinsichtlich der vorgesehenen DV prüfen, ob jeweilige Zweckfestlegung (nach § 28 I S. 2 BDSG) die geplante Zusammenlegung gestattet und hierfür ein berechtigtes Interesse vorliegt (§ 28 II BDSG i.V.m. § 28 I Nr. 2 BDSG)
  → Nachweis für Erforderlichkeit & Abwägung

2.3 Kundenspezifische Datenanalysen (2)

- Zuspeicherung der Daten für Bestandskunden aber an sich zulässig (wg. § 28 III S. 3 BDSG)
- Durchführende Beschäftigte sind auf das Datengeheimnis zu verpflichten (§ 5 BDSG)
- Für das CRM-System sind ausreichende technische und organisatorische Maßnahmen zu ergreifen (§ 9 BDSG samt Anlage)
- CRM-System stellt eigenes Verfahren im Verfahrensverzeichnis dar

2.4 Auftragsdatenverarbeitung Call-Center

Aufgabe:

- Ein Call-Center wertet für ihre Auftraggeber Daten im 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!

2.4 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)

2.4 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)

2.5 Auswertung öffentlicher Daten für Werbezwecke

Aufgabe:

- Ein Unternehmen möchte Angaben aus einem sozialen Netzwerk auswerten, um daraus Kenntnisse zu gewinnen, ob eigene Kunden (alles Endverbraucher), die im sozialen Netzwerk mit einem eigenen Profil vertreten sind, anhand von deren allgemein sichtbaren Angaben gezielter beworben werden können. **Ist diese Auswertung** der veröffentlichten Daten zu Werbezwecken **zulässig?** Begründen Sie Ihre Antwort!

2.5 Auswertung öffentlicher Daten für Werbezwecke (1)

- Soziales Netzwerk = privatrechtliche Plattform, mit der die jeweiligen Nutzer ein rechtsgeschäftliches Schuldverhältnis eingegangen sind
  → Soziales Netzwerk weist i.d.R. Nutzungsbedingungen auf
  → Soziales Netzwerk geht mit personenbezogenen Nutzungsdaten um und beschreibt daher datenschutzrechtliche Aspekte in einer eigenen Datenschutzerklärung
- Nur allgemein sichtbare Angaben der Nutzer werden ausgewertet
  → Öffentlich zugängliche Daten dürfen nach § 28 Abs. 1 Nr. 3 BDSG für eigene Geschäftszwecke verwendet werden!
  → Ausschluss an Verwendung nur gegeben, wenn Betroffeneninteresse offensichtlich dagegen spricht
  → Gründe gegen Verwendung: Offenbarung der Daten innerhalb eines bestimmten Kontextes (soziales Netzwerk), aber: veröffentlichte Daten allgemein zugänglich, d.h. ohne Zugriffsschutz abrufbar

2.5 Auswertung öffentlicher Daten für Werbezwecke (2)

- Nur allgemein sichtbare Angaben der Nutzer werden ausgewertet (Forts.)
  → Daten zulässig veröffentlicht, wenn diese vom Betroffenen selbst eingestellt wurden
  → keine Daten auswerten, die von anderen Nutzern über die Betroffenen eingestellt wurden! → **führt sonst zur Unzulässigkeit!**
  → Daten dürfen nur dann ausgewertet werden, wenn man sich zum Abruf der Daten nicht am sozialen Netzwerk anmelden muss (sonst potenzieller Verstoß gegen Nutzungsbedingungen und ggf. überwiegender Ausschlussgrund für Betroffene) → **werden Daten erst nach entsprechender Anmeldung am sozialen Netzwerk ausgewertet, wäre Datenverwendung unzulässig!**
  → nur Daten auswerten, die über Suchmaschinen oder öffentlich verfügbare Suchfunktionen des sozialen Netzwerks abrufbar sind

2.5 Auswertung öffentlicher Daten für Werbezwecke (3)

- Ausgewertet werden nur Daten von und über Betroffene, die bereits zu den Bestandskunden gehören
- Auswertungsdaten sollen zu Werbezwecken verwendet werden!
  → Voraussetzungen aus § 28 Abs. 3 BDSG zu beachten
- Auswertungsdaten sollen lediglich zum bestehenden Datensatz über Betroffene hinzugespeichert werden
  → Zuspeicherung von weiteren Daten nur zulässig, wenn Voraussetzungen aus § 28 Abs. 3 S. 3 BDSG erfüllt ist
  → Betroffenendaten müssen unter das Listenprivileg aus § 28 Abs. 3 S. 2 Nr. 1 BDSG fallen
  → öffentlich zugängliche Quellen insoweit eingeschränkt auf allgemein zugängliche Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnisse
  → soziales Netzwerk kein derartiges Verzeichnis → **unzulässig!**