Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2018:

Kundendatenschutz (3)

5.1 Cookies

Aufgabe:

- Auf einem Webportal sollen anhand der Identifizierung des Nutzers durch gesetzte Cookies gezielt Werbebotschaften eingeblendet werden, in denen Produkte beworben werden, die von Kunden mit vergleichbarem Kaufverhalten erworben wurden. Unter welchen Voraussetzungen ist das zulässig? Begründen Sie Ihre Antwort!

5.1 Cookies (1)

- Webportal = Telemediendienst → TMG einschlägig
- Cookies setzen eine elektronische Einwilligung der Nutzer unter Berücksichtigung von § 13 Abs. 2 TMG voraus; dabei ist der Nutzer auf sein Widerspruchsrecht hinzuweisen (§ 13 Abs. 3 TMG)
- Ein Diensteanbieter darf für Werbezwecke Nutzungsprofile erstellen, sofern der Nutzer diesem nicht widersprochen hat (§ 15 Abs. 3 TMG); auf das Widerspruchsrecht ist in der Datenschutzerklärung nach § 13 Abs. 1 TMG hinzuweisen
- Zur Erstellung der Nutzungsprofile sind Pseudonyme zu verwenden → laut Aufgabenstellung ist nur das charakteristische Käuferverhalten, welches über das Webportal erfolgt, relevant
  → Die Cookie-ID ist ein derartiges Pseudonym
  → Vergleich zu Werbezwecken ohne Bezug zu Träger des Pseudonyms zulässig!

5.1 Cookies (2)

- Nutzer kann jederzeit seine Einwilligung einsehen, da diese lokal auf seinem Rechner gespeichert ist
- Nutzer kann jederzeit seine Einwilligung widerrufen, indem er das Cookie löscht
- Sollen Daten aus Cookies ausgelesen und in Bezug auf gespeichertes Kaufverhalten ausgewertet werden, darf dabei kein Personenbezug hergestellt werden → <u>Datamining ohne unmittelbaren Personenbezug</u> (sowohl hinsichtlich der IP-Adresse, die zu dem Cookie gehört als auch zu dem Portalnutzer!)
- Da keine Werbungen (elektronisch) versandt werden, sondern nur als Werbebotschaften im Webportal angezeigt werden, liegt auch keine unzumutbare Belästigung nach § 7 Abs. 1 UWG vor
- Werbebotschaft = Werbebanner
  → <u>Online Behavioural Advertising</u>

5.2 Datenschutz-Erklärung zur Big-Data-Analyse

Aufgabe:

- Was ist aus datenschutzrechtlicher Sicht zu beachten, wenn ein Unternehmen alle gespeicherten Daten über Ihre Bestands-kunden einer Big Data Analyse unterziehen möchte? Erstellen Sie hierzu eine geeignete Datenschutzerklärung im Sinne von Art. 14 EU-DSGVO!

5.2 Datenschutz-Erklärung zur Big-Data-Analyse (1)

Vorbemerkungen:

- Big Data = Verarbeitung umfangreicher Datenmengen
- Datensammlungen weisen i.d.R. unstrukturierte Daten auf, die erst mittels Big Data Processing strukturiert werden sollen
- Ziel ist i.d.R. strukturelle Informationen zu gewinnen, die mit recht hoher Wahrscheinlichkeit Zukunftsprognosen zulassen
- Wurden Datensätze ursprünglich zu unterschiedlichen Zwecken erhoben, ist darauf zu achten, dass die neu verfolgten Zwecke noch mit den ursprünglichen vereinbar sind, sonst ist eine Anonymisierung nötig
- Anhand der Datensammlung darf keine automatisierte Einzelentscheidung vorgenommen werden
- Da die Daten für Big Data Analysen i.d.R. nicht beim Betroffenen direkt erhoben werden, sondern aus anderen Datensenken stammen, sind Betroffene nach Art. 14 EU-DSGVO zu informieren

5.2 Datenschutz-Erklärung zur Big-Data-Analyse (2)

Datenschutz-Information nach Art. 14 EU-DSGVO:

Name und Kontaktdaten des Verantwortlichen:

Anschrift: XY GmbH, Musterstr. 1, 12345 Musterstadt
Tel: 01234/56789-0, Mail: info@xy-gmbh.de
Datenschutzbeauftragter: Manfred Mustermann
Tel: 01234/56789-9, Mail: datenschutz@xy-gmbh.de

Zwecke der Verarbeitung und Rechtsgrundlage:

Zweck: Anonymisierte Auswertung der Bestandsdaten zur Ermittlung statistischer Zusammenhänge; keine automatisierte Entscheidung
Rechtsgrundlage: Art. 6 Abs. 1 lit. f EU-DSGVO mit folgenden berechtigten Interessen des Verantwortlichen:

° Transparenz über geschäftswichtige Zusammenhänge
° Qualitätssteigerung
° Verbesserung betrieblicher Abläufe
° Förderung des Absatzes und der Nachfrage

5.2 Datenschutz-Erklärung zur Big-Data-Analyse (3)

Datenschutz-Information nach Art. 14 EU-DSGVO: Fortsetzung

Datenkategorien und Datenherkunft:
Bestandsdaten aus CRM, Finanzbuchhaltung und Newsletterverfahren

Empfänger:
interne Stellen zur Aufgabenerledigung
keine Übermittlung in Drittland

Speicherdauer:
Nach Durchführung der Anonymisierung unbegrenzt

Betroffenenrechte:
Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit und Beschwerde bei der Aufsichtsbehörde (per Mail an beschwerde@datenschutzaufsicht.de)

5.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung I

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

5.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung II

Aufgabe: (Fortsetzung)

- Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer Datenschutz-Folgenabschätzung (gem. Art. 35 EU-DSGVO) sehen (unter Berücksichtigung der Bußgeldbestimmungen und Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten), schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß nächstehender 3x3-Risk-Map. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

5.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (1)

1) Ermittlung potenzieller Datenschutzrisiken:

- Lesender & schreibender Zugriff des Web-Portals auf CRM-System
  1. Unbeschränkter Zugriff auf alle CRM-Daten → Gefahr: Unbefugte Offenlegung & Unrechtmäßige oder unbeabsichtigte Veränderung (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)
- Benutzerkennung via fortlaufender Nummer & freie Passwortwahl
  2. Enumerative Zugangsdaten → Gefahr: kein unmittelbarer Schaden
  3. Mangelnder Zugriffsschutz bei geringer Passwortgüte → Gefahr: Unbefugter Zugang (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)
- Bestätigungsmail für durchgeführte Bestellungen
  4. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden → Gefahr: kein unmittelbarer Schaden
- Einsicht in Bestellhistorie via Web-Portal
  5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil → Gefahr: Umfassendes Profiling durch unzureichende Maßnahmen des Web-Portals unzureichend geschützt (formaler Verstoß, da durch diese DSFA ja behandelt)

5.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (2)

2) Abschätzung der Eintrittsstufe:

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. Enumerative Zugangsdaten: Gefahreintritt sicher, da entsprechendes Ausprobieren voraussetzungslos möglich ist
3. 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)
4. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden: Gefahreintritt nur möglich, da Angreifer erst noch den Verbindungspfad ermitteln muss
5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil: Gefahreintritt sicher, aufgrund der Voraussetzungen aus 2. & 3.

5.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (3)

Wahrscheinlichkeit			
3	**2.**	**5.**	**3.**
2			**1.**
1	**4.**		
Schaden	1	2	3

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

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

5.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (4)

3) Handlungsempfehlung:

1. Unbeschränkter Zugriff auf alle CRM-Daten
   → Datenvalidierung sicherstellen (SQL-Injection verhindert) & schreibenden Zugriff auf CRM-System unterbinden
2. Enumerative Zugangsdaten
   → Benutzerkennung frei wählen lassen
3. Mangelnder Zugriffsschutz bei geringer Passwortgüte
   → Mindestvorgaben für Passwortgüte festlegen (Komplexität, Länge)
4. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
   → akzeptierbar, wenn Verbindungspfad nicht ermittelbar ist und ein Angreifer nicht als Man-in-the-Middle zwischenschalten kann
5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil
   → nach Änderung zu 2. & 3. ggf. akzeptierbar

5.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (5)

Anmerkung:

- Die Angabe der Punkte aus Art. 35 Abs. 7 EU-DSGVO ist bei der Durchführung von Datenschutz-Folgenabschätzungen verpflichtend
  - ° auf systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen hier verzichtet, da dies nicht eindeutig aus der Aufgabenstellung hervor geht

5.4 Datenschutzmanagement

Aufgabe:

- Welche Prozesse hat ein Unternehmen zum Datenschutzmanagement aufgrund der datenschutzrechtlichen Bestimmungen aus EU-DSGVO & TMG umzusetzen?
  Hinweis: Orientieren Sie sich dabei an den Aufgaben, die der Datenschutzbeauftragte in Zusammenarbeit mit anderen Stellen im Unternehmen im Zusammenhang mit dem Kundendatenschutz zu erfüllen hat.

5.4 Datenschutzmanagement (1)

Prozesse zum Management des Kundendatenschutzes nach EU-DSGVO:

Alle nachstehenden Angaben sind nicht nur auf Kundendatenschutz beschränkt.

- **Führung des Verzeichnisses von Verarbeitungstätigkeiten** nach Art. 30 Abs. 1 EU-DSGVO durch Verantwortliche bzw. nach Art. 30 Abs. 2 EU-DSGVO durch Auftragsverarbeiter
- **Benennung eines Datenschutzbeauftragten** nach Art. 37 Abs. 1 EU-DSGVO
- **Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten** nach Art. 37 Abs. 7 EU-DSGVO
- **Datenschutz-Folgenabschätzung** von Verarbeitungen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aufweisen können nach Art. 35 Abs. 1 EU-DSGVO unter Beteiligung des Datenschutzbeauftragten nach Art. 35 Abs. 2 EU-DSGVO
  → neue Verfahren beim Datenschutzbeauftragten anmelden!
  → Angaben aus Verzeichnis von Verarbeitungstätigkeiten melden (inkl. geplanter Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO)
  → Angaben über verfolgte berechtigte Interessen, Datenfluss und Zugriffsrollen
  → Rat des Datenschutzbeauftragten einholen! (Art. 39 Abs. 1 lit. c EU-DSGVO)
  → Bewertung Notwendigkeit, Verhältnismäßigkeit & Risiken

5.4 Datenschutzmanagement (2)

Prozesse zum Management des Kundendatenschutzes n. EU-DSGVO: 1. Forts.

- **Regelkontrolle zur Überwachung** der Einhaltung datenschutzrechtlicher Vorschriften nach Art. 39 Abs. 1 lit. b EU-DSGVO
  → Datenschutzbeauftragten rechtzeitig über bestehende & geplante Verarbeitung unterrichten nach Art. 38 Abs. 1 EU-DSGVO!
  → i.d.R. durch Verzeichnis von Verarbeitungstätigkeiten
  → unter Berücksichtigung der Risiken nach Art. 39 Abs. 2 EU-DSGVO
- **Unterrichtung und Beratung der** bei der Verarbeitung personenbezogener Daten **tätigen Personen über ihre datenschutzrechtlichen Pflichten** nach Art. 39 Abs. 1 lit. a EU-DSGVO:
  → Schulungen & Sensibilisierungen nach Art. 39 Abs. 1 lit. b EU-DSGVO
  → Informationsschriften / Merkblätter
  → Belehrungen
  → unter Berücksichtigung der Risiken nach Art. 39 Abs. 2 EU-DSGVO
- **Unterstützung des Datenschutzbeauftragten** durch erforderliches Hilfspersonal sowie Räume, Einrichtungen, Geräte, Mittel und Fortbildungen nach Art. 38 Abs. 2 EU-DSGVO
- **Bearbeitung von Betroffenenanliegen** nach Art. 38 Abs. 4 EU-DSGVO

5.4 Datenschutzmanagement (3)

Prozesse zum Management des Kundendatenschutzes n. EU-DSGVO: 2. Forts.

- **Festlegung geeigneter technischen und organisatorischer Maßnahmen** nach Art. 32 EU-DSGVO unter Berücksichtigung der Risiken nach Art. 24 Abs. 1 EU-DSGVO
- **Nachweisführung zur Einhaltung der EU-DSGVO** nach Art. 24 Abs. 1 EU-DSGVO
- **Regelmäßige Überprüfung und Aktualisierung der Schutzvorkehrungen** nach Art. 24 Abs. 1 EU-DSGVO
- **Erlass geeigneter Datenschutzrichtlinien** nach Art. 24 Abs. 2 EU-DSGVO
- **Auswahl geeigneter Auftragnehmer, deren Beratung und Überprüfung** nach Art. 28 Abs. 1 und Art. 39 Abs. 1 lit. a & b EU-DSGVO
- **Unterstützung bei den Abwägungen** nach Art. 6 Abs. 1 lit. f EU-DSGVO
- **Etablierung wirksamer Verfahren zur Beachtung von Werbewidersprüchen** nach Art. 21 Abs. 3 EU-DSGVO
- **Unterstützung bei der Meldung von Datenpannen** nach Art. 33 EU-DSGVO
- **Zusammenarbeit mit der Aufsichtsbehörde** nach Art. 39 Abs. 1 lit. d EU-DSGVO
- **Unterstützung bei der Bestimmung erforderlicher Sorgfalt** zur Vermeidung von Schadensersatz nach Art. 82 Abs. 3 EU-DSGVO

5.4 Datenschutzmanagement (4)

Prozesse zum Management des Kundendatenschutzes nach **TMG**:

- **Unterstützung bei der Beachtung der Zweckbindung bei Einsatz von Telemedien** (§ 12 TMG)
- **Unterstützung bei der Formulierung der für den Nutzer <u>jederzeit abrufbaren</u> Datenschutzerklärung** (§ 13 Abs. 1 TMG) **bzw. der Informationen nach Art. 13 und 14 EU-DSGVO**
- **Unterstützung bei der Festlegung der spezifischen technischen und organisatorischen Maßnahmen** nach dem Telemedienrecht (§ 13 Abs. 4 TMG → Löschung personenbezogener Daten nach Beendigung des Dienstes & wirksame Pseudonymisierung)
- **Unterstützung bei der Behandlung einer Datenpanne** (§ 15a TMG), allerdings i.V.m. Art. 33 und 34 EU-DSGVO (statt § 42a BDSG)

5.5 Aufgaben Kundendatenschutz I

Aufgabe:

- Bei einem Unternehmen ist unter Verwendung des **RACI-Modells** festzulegen, welche Stelle welche Aufgabe im Rahmen der Gewährleistung des Kundendatenschutzes zu erfüllen hat. Erstellen Sie eine Übersicht, in der Sie typische Aufgaben zur Gewährleistung des Kundendatenschutzes folgenden Stellen zuweisen:
  ° Geschäftsführer (in der Funktion als Vertreter des Verantwortlichen)
  ° Leiter Vertrieb und Marketing (hauptverantwortlich für Prozesse zur Kundendatenverarbeitung)
  ° Datenschutzbeauftragter
  ° Mitarbeiter Vertrieb und Marketing (ausführende Stelle)
  Berücksichtigen Sie in Ihrer Lösung nur folgende Verfahren:
  ° CRM
  ° Direktmarketing (Werbekampagne, Newsletter)
  ° Anreizsystem (Gewinnspiel, Rabattsystem)

5.5 Aufgaben Kundendatenschutz II

Aufgabe:

- Konzentrieren Sie sich dabei auf das Wesentliche. Beachten Sie bei Ihrer Lösung, dass niemand eine Aufgabe umzusetzen hat, der diese Aufgabe zugleich zu genehmigen hat.
  Hinweis:
  *Beim **RACI-Modell** gibt es vier Rollen, nämlich*
  R = Responsible → *Umsetzung einer Aufgabe*
  A = Accountable → *Genehmigung einer Aufgabe*
  C = Consulted → *Anhörungsinstanz bei einer Aufgabe*
  I = Informed → *Mitteilungsempfangsinstanz bei einer Aufgabe*

5.5 Aufgaben Kundendatenschutz (1)

Datenschutz beim CRM [vgl. Aufgabe 3.1]	GF	V. & M. Leiter	DSB	V. & M. MA
Dokumentation aller verfolgten Haupt- und Nebenzwecke, der verfolgten berechtigten Interessen und der getroffenen Sicherheits-Maßnahmen	A	R	C	I
Bereitstellung der nötigen Informationen für Betroffene (Art. 14 DSGVO)		A	C	R
Löschen personenbezogener CRM-Daten nach Ablauf der Speicherfrist		A	C	R
Prüfung der Angemessenheit der getroffenen Sicherheits-Maßnahmen		A	R	
Prüfung der Einhaltung der EU-DSGVO-Vorgaben	A	C	R	

Datenschutz beim Direktmarketing (Werbekampagne, Newsletter) [vgl. Aufgaben 3.2 & 3.4]	GF	V. & M. Leiter	DSB	V. & M. MA
Dokumentation aller verfolgten Haupt- und Nebenzwecke, der verfolgten berechtigten Interessen und der getroffenen Sicherheits-Maßnahmen	A	R	C	I
Dokumentation eingegangener Einwilligungen und Werbewidersprüche		A		R
Prüfung, dass Werbekampagne nur in Bezug auf bisherige Kaufhistorie erfolgt		A		R
Prüfung, dass für Newsletter benötigte Einwilligung vorliegt		A		R
Aussendung von Werbungen nur an Adressaten, die nicht widersprochen haben, und über die zugelassenen Kommunikationswege		A		R
Löschen personenbezogener Werbe-Daten nach Ablauf der Speicherfrist		A	C	R
Prüfung der Einhaltung der EU-DSGVO-Vorgaben	A	C	R	

5.5 Aufgaben Kundendatenschutz (2)

Datenschutz bei Anreizsystemen (Gewinnspiel, Rabattsystem) [vgl. Aufgaben 4.1 & 4.2]	GF	V. & M. Leiter	DSB	V. & M. MA
Dokumentation aller verfolgten Haupt- und Nebenzwecke, der verfolgten berechtigten Interessen und der getroffenen Sicherheits-Maßnahmen	A	R	C	I
Bereitstellung der nötigen Informationen für Betroffene (Art. 13 DSGVO, beim Gewinnspiel zudem der Teilnahmebedingungen)		A	C	R
Dokumentation eingegangener Einwilligungen (Gewinnspiele) und vertraglichen Vereinbarungen (Rabattsystem)		A		R
Ausschüttung der Gewinne über die zugelassenen Kommunikationswege		A		R
Information der Teilnehmer am Rabattsystem über den aktuellen Stand		A		R
Löschen personenbezogener Anreiz-Daten nach Ablauf der Speicherfrist		A	C	R
Prüfung der Einhaltung der EU-DSGVO-Vorgaben	A	C	R	