# Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2019:

Kundendatenschutz (4) &
Datenschutzmanagement

# 5.1 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.*

# 5.1 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

# 5.1 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

# 5.1 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

# 5.1 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 jederzeit abrufbaren 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)

# 5.2 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.
  Welche technischen und organisatorischen Maßnahmen sind für diese Verfahren im Rahmen der Kundendatenverwaltung zwingend, damit keine besonderen Risiken für die Rechte und Freiheiten der Betroffenen davon ausgehen können? Begründen Sie Ihre Antwort!

# 5.2 Schutzmaßnahmen (1)

**Schutz des Web-Portals**:

- 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

# 5.2 Schutzmaßnahmen (2)

**Schutz des Web-Portals**: 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
  → 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 Netz-werksegmentierung und -segregation

# 5.2 Schutzmaßnahmen (3)

**Schutz des Buchhaltungssystems**:

- 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

# 5.2 Schutzmaßnahmen (4)

**Schutz des Buchhaltungssystems**: Forts.

- 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 Datenschutzverletzung
- Protokollierung der Datenübertragung (z.B. ans CRM-System) im Rahmen der Überwachung der Kundenhistorie

# 5.2 Schutzmaßnahmen (5)

**Schutz des CRM-Systems**:

- Gewährleistung der Zweckbindung
  → keine unzulässige Verknüpfung von Daten mit verschiedenen Zwecken
- Wirksamer Zugriffsschutz (i.d.R. andere Zugriffsberechtigte als beim Buchführungssystem wg. Segregation of Duties!)
- Bereitstellung von anonymisierten Reports (→ Vermeidung von Drill-Down-Funktionen)
  → Grundsatz der Datenminimierung (Privacy by Design)
- Regelmäßige Kontrollen, ob eine unzulässige Datenanreicherung stattfand
  → Vermeidung einer ungewollten Erhöhung des Schutzbedarfs

# 5.2 Schutzmaßnahmen (6)

**Schutz des CRM-Systems**: Forts.

- Protokollierung über Anfertigung spezifischer Auswertungen & Beschränkung möglicher Auswertungsfunktionen
  → Prävention unzulässiger Datenverwendungen
- Sperrfeld zur Berücksichtigung von Werbewidersprüchen
  → Umsetzung sowohl datenschutzrechtlicher als auch wettbewerbsrechtlicher Verstöße durch Nichtbeachtung des jeweiligen Widerspruchsrechts

# 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:**

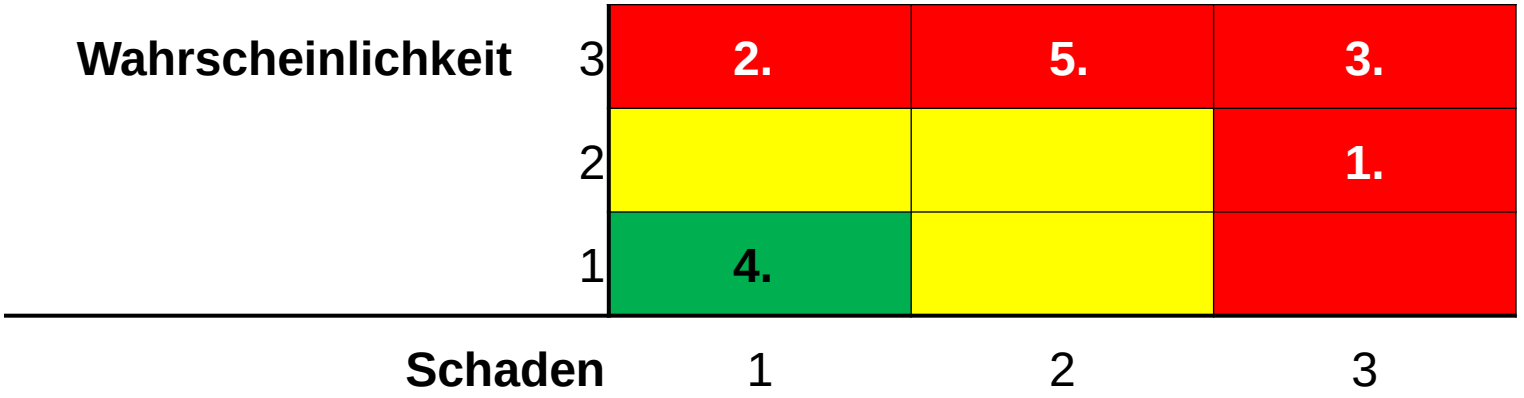
- Lesender & schreibender Zugriff des Web-Portals auf CRM-System
  1. Unbeschränkter Zugriff auf alle CRM-Daten → Gefahr: Unbefugte Offenlegung & Unrechtmäßige oder unbeabsichtigte Veränderung (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)
- Benutzerkennung via fortlaufender 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 Auspro-bieren 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)




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

| **Wahrscheinlichkeit:**<br>**Eintritt einer Verletzung des Schutzes personenbezogener Daten** | **Schaden:**<br>**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/Meldepflicht) |

# 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 nach Aufgabenstellung nicht zwingend verlangt

# 5.4 Vorkehrungen gegen hohe Risiken

**Aufgabe:**

- Geben Sie fünf frei wählbare Beispiele beim Umgang mit personenbezogenen Kundendaten an, bei denen grundsätzlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen bestehen kann und skizzieren Sie zu treffende Vorkehrungen, die bei diesen Beispielen durch den Verantwortlichen getroffen werden müssen, um entweder die Höhe eines potenziellen Schadens oder die Eintrittswahrscheinlichkeit eines solchen Schadens entweder vermeiden oder zumindest ausreichend mindern zu können. Begründen Sie Ihre Antwort und geben Sie insbesondere an, wie die von Ihnen vorgeschlagene Vorkehrung hinsichtlich des Risikos wirkt!

# 5.4 Vorkehrungen gegen hohe Risiken (1)

**1. Beispiel: Erstellung eines umfassenden Kundenprofils unter Einbeziehung von Gesundheitsdaten (zum Vertrieb von Vitamindrinks)**

- **Abschätzung Schaden: hoch!** Gesundheitsdaten besonders schützenswert und nur unter den Voraussetzungen aus Art. 9 Abs. 2 EU-DSGVO verwendbar
- **Abschätzung Eintrittswahrscheinlichkeit: mittel!** Qualitativ hochwertige Profildaten für Angreifer ausreichend interessant, muss aber erst mal Zugriff auf Daten erhalten
- **Vorkehrung**: Pseudonymisierung bei Verknüpfung zu Gesundheitsdaten und Clusterung zu charakteristischen Vitamindrinktypen
- **Wirkung: Minderung Schaden auf mittel!** Angreifer muss zugleich Pseudonymisierung brechen, um Daten missbrauchen zu können

# 5.4 Vorkehrungen gegen hohe Risiken (2)

**2. Beispiel: Vereinbarung der Zahlungsbedingungen in ausschließlicher Abhängigkeit zum Scoringwert der betroffenen Person**

- **Abschätzung Schaden: hoch!** Bei ausschließlicher Abhängigkeit zum Scoringwert Verstoß gegen Art. 22 Abs. 1 EU-DSGVO, bußgeldbewährt nach Art. 83 Abs. 5 lit. b EU-DSGVO
- **Abschätzung Eintrittswahrscheinlichkeit: hoch!** Bei automatisierter Einzelentscheidung ist der Eintritt einer potenziell ungerechtfertigten Benachteiligung betroffener Personen unvermeidbar
- **Vorkehrung**: Neben zusätzlich zu gebender Information aus Art. 13 Abs. 2 lit. f EU-DSGVO und der Berücksichtigung der Vorgaben aus Art. 22 EU-DSGVO (Recht auf Erwirkung des Eingreifens einer Person beim Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung) regelmäßige Überprüfung anhand Eingaben der betroffenen Personen
- **Wirkung: Minderung Schaden auf mittel und Eintrittswahrscheinlichkeit auf mittel!** Berücksichtigung aller Vorgaben aus Art. 22 EU-DSGVO verhindert unmittelbares Bußgeldrisiko, durch Vorkehrungen zugleich systematische Benachteiligung reduziert

# 5.4 Vorkehrungen gegen hohe Risiken (3)

**3. Beispiel: Für neuen Zweck Verknüpfung von Profildaten aus unterschiedlichen Datensammlungen zu nicht miteinander vereinbaren Zwecken**

- **Abschätzung Schaden: hoch!** Verstoß gegen Grundsatz aus Art. 5 Abs. 1 lit. b EU-DSGVO, bußgeldbewährt nach Art. 83 Abs. 5 lit. a EU-DSGVO
- **Abschätzung Eintrittswahrscheinlichkeit: hoch!** Unterschiedslose Verknüpfung aller vorhanden Daten führt sicher zur Datenschutzverletzung, da folglich dann keine angemessenen Schutzvorkehrungen getroffen wurden
- **Vorkehrung**: Wo die Zwecke miteinander vereinbar sind, angemessenen rollenbasierten Zugriffsschutz implementieren, um Missbrauchspotenzial zu reduzieren, und sonst Daten vorher mindestens pseudonymisieren und erst danach mit Wahrscheinlichkeitsaussagen kombinieren (Big Data Verfahren)
- **Wirkung: Minderung Schaden auf mittel und Eintrittswahrscheinlichkeit auf mittel!** Wenn Zwecke miteinander vereinbar sind und nur Wahrscheinlichkeiten aus Big Data Analyse hinzugespeichert wird, wo die Zwecke nicht miteinander vereinbar sind, ist Bußgeldrisiko reduziert; durch Zugriffsschutz neben Pseudonymisierung angemessene Maßnahme getroffen

# 5.4 Vorkehrungen gegen hohe Risiken (4)

**4. Beispiel: Aufzeichnung der Bewegungsdaten im Supermarkt mit Analyse der Haltedaten des Einkaufswagens und Abgleich mit Kassendaten und Videoüberwachungsdaten (zur Abschätzung von Geschlecht und Alter des Einkäufers)**

- **Abschätzung Schaden: niedrig!** Kein unmittelbarer Schaden für Rechte und Freiheiten betroffener Personen
- **Abschätzung Eintrittswahrscheinlichkeit: hoch!** Verletzung der Zweckbindung der Videoüberwachungsdaten
- **Vorkehrung**: Befragung der Einkäufer an der Kasse für statistische (Big Data) Zwecke mit Angabe aller relevanten Informationen (analog zur Postleitzahlen-abfrage)
- **Wirkung: Minderung Eintrittswahrscheinlichkeit auf mittel!** Erhebung der Big Data Datensammlung auf Basis einer Einwilligungserklärung

# 5.4 Vorkehrungen gegen hohe Risiken (5)

**5. Beispiel: Dauerhafte Aufzeichnung von Schaufensterpassanten und Auswertung, wie lange vor welchem Ausstellungsstück von welchem Personentyp gehalten wurde**

- **Abschätzung Schaden: niedrig!** Kein unmittelbarer Schaden für Rechte und Freiheiten betroffener Personen
- **Abschätzung Eintrittswahrscheinlichkeit: hoch!** Verletzung der Zweckbindung der Videoüberwachungsdaten
- **Vorkehrung**: Unterlassen der unzulässigen Auswertung der Videodaten bzw. Unterlassen der Videoaufzeichnung
- **Wirkung: Vermeidung Risiko!** Durch Unterlassen besteht kein Risiko mehr

# 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 2.5] | 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 (Newsletter, Werbekampagne) [vgl. Aufgaben 3.1 & 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 | |