Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2018:

Kundendatenschutz (1)

3.1 CRM-System

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!

3.1 CRM-System (1)

- Unternehmen = nicht-öffentliche Stelle
- CRM-System = System zur Kunden**bewertung** von wirtschaftlicher Lage, persönlicher Vorlieben, (Kauf-) Interessen, (Zahlungs-) Zuverlässigkeit & (Bestell- und Reklamations-) Verhalten
  → Profiling nach Art. 4 Nr. 4 EU-DSGVO
  → Datenschutz-Folgenabschätzung nötig nach Art. 35 Abs. 3 lit. a EU-DSGVO
  → Verhinderung einer Verarbeitung mit hohem Risiko für die Rechte und Freiheiten der Betroffenen
  → umfassende Schutzmaßnahmen nach Art. 32 EU-DSGVO erforderlich!

3.1 CRM-System (2)

- Nach Art. 35 Abs. 7 EU-DSGVO ist in der Datenschutz-Folgenabschätzung zumindest Folgendes zu behandeln:
  - Beschreibung der geplanten Verarbeitungsvorgänge
    → Detaillierte Festlegung der Verarbeitungsschritte
  - Verfolgte Zwecke und berechtigte Interessen
    → für jeden Schritt muss ein legitim verfolgten Zweck bestehen
    → bei berechtigten Interessen Abwägung darstellen, um Widerspruchsrechte der Betroffenen nach Art. 21 Abs. 1 EU-DSGVO abwehren zu können
  - Bewertung zur Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf die verfolgten Zwecke
  - Zur Bewältigung der Risiken geplante technische und organisatorische Abhilfemaßnahmen darstellen

3.1 CRM-System (3)

- Die Grundsätze aus Art. 5 Abs. 1 EU-DSGVO müssen für das CRM-System eingehalten werden
  → u.a. Datenminimierung & Speicherbegrenzung beachten
  → Import aus anderen Datenquellen muss mit den dafür ursprünglich festgelegten Zwecken vereinbar sein, sonst wird eine Informationspflicht ausgelöst nach Art. 14 Abs. 4 EU-DSGVO
  → sinnvollerweise dies bereits bei Datenschutz-Folgenabschätzung berücksichtigen
- Sofern ein DSB benannt wurde, diesen bei der Datenschutz-Folgenabschätzung anhören
- CRM-System ist in das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO aufzunehmen

3.2 Werbekampagne

Aufgabe:

- Ein Unternehmen möchte eine Werbekampagne bei seinen Bestandskunden (Endverbraucher) durchführen und diesen in Abhängigkeit zu bisher erworbenen Produkten eine gezielte Werbung per Mail zusenden. Die Mail-Adressen wurden von den Kunden im Rahmen der Geschäftsbeziehung mitgeteilt. Alle relevanten Daten samt der Kundenhistorie finden sich im CRM-System. Wie muss das Unternehmen vorgehen, um die geplante Werbekampagne durchführen zu können?

3.2 Werbekampagne (1)

- Eine Werbekampagne per E-Mail setzt voraus, dass es sich in nicht um eine unzumutbare Belästigung im Sinne von § 7 Abs. 2 Nr. 3 UWG handeln darf.
- Dies ist nach § 7 Abs. 3 UWG dann nicht der Fall, wenn
  - das Unternehmen die Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten hat (das ist nach Aufgabenstellung der Fall)
  - das Unternehmen die Mail-Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet (das ist ja ausdrücklich das Ziel der Werbekampagne)
    → Werbekampagne darf sich nur auf ähnliche Produkte des Unternehmens beziehen!
    → Werbekampagne orientiert sich an Produktgruppen
    → entsprechende Auswertung des CRM-Systems nötig!

3.2 Werbekampagne (2)

- Dies ist nach § 7 Abs. 3 UWG dann nicht der Fall, wenn (Forts.)
  - der Kunde der Verwendung seiner Mail-Adresse zu Werbezwecken nicht widersprochen hat
    → vor Aussendung einer entsprechenden Werbemail prüfen!
    → im CRM-System eingehende Widersprüche speichern!
  - der Kunde bei der Erhebung der Mail-Adresse (ebenfalls nach Art. 21 Abs. 4 EU-DSGVO) und (!) bei jeder Verwendung klar und deutlich auf sein Widerspruchsrecht hingewiesen wird
    → ein entsprechender Hinweissatz in den Mail-Text der Werbemail ausdrücklich aufnehmen

3.2 Werbekampagne (3)

- Datenschutzrechtlich basiert Werbung auf der Verfolgung berechtigter Interessen nach Art. 6 Abs. 1 lit. f EU-DSGVO (laut ErwG 47), nicht mehr auf der Einwilligung (außer Newsletter) → bei Design der Werbekampagne etwaige widerstreitende Interessen der Betroffenen berücksichtigen!
- Eingesetzte Systeme zur Werbekampagne (CRM-System und Mail-System) müssen angemessen im Sinne von Art. 32 EU-DSGVO geschützt sein.
- Werbekampagne ist in Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO (in allgemeiner Form, d.h. nicht für jede durchgeführte Kampagne wieder auf‘s Neue, soweit nicht kampagnen-spezifisch bei der Abwägung unterschiedlich vorzugehen ist, dann Abwägung jeweils entsprechend konkretisieren) aufgenommen werden

3.3 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 sowie ein Lagerverwaltungs-System zur Steuerung, Zwischenlagerung und Bereitstellung für den Versand hergestellter Güter mittels RFID-Chips.
  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!

3.3 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

3.3 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

3.3 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

3.3 Schutzmaßnahmen (4)

Schutz des Buchhaltungssystems:

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

3.3 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

3.3 Schutzmaßnahmen (6)

Schutz des CRM-Systems:

- 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

3.4 Newsletter

Aufgabe:

- Ein Unternehmen möchte an seine Bestandskunden einen via E-Mail zu verschickenden Newsletter zustellen. Wie muss es hierzu vorgehen, um sowohl die datenschutzrechtlichen, telemedienrechtlichen und wettbewerbsrechtlichen Anforderungen zu erfüllen? Begründen Sie Ihre Antwort!

3.4 Newsletter (1)

Datenschutzrechtliche Anforderungen:

- Analog zur Werbekampagne (→ Aufgabe 3.2), aber mit dem Unterschied, dass im Newsletter auch zu Inhalten Informationen verschickt werden dürfen, die nicht unmittelbar mit der Bestellhistorie zu tun haben
  → eigenständiges Verfahren, das in Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO aufzunehmen ist
- Newsletter darf nicht an Bestandskunden versandt werden, die diesem widersprochen haben (Art. 21 Abs. 3 EU-DSGVO)
  → Prüfung, ob Widerspruch vorliegt
  → Eingesetztes System zu Planung und Versand von Newslettern muss Sperrfeld aufweisen, in das eingegangene Widersprüche eingetragen werden

3.4 Newsletter (2)

Wettbewerbsrechtliche Anforderungen:

- Analog zur Werbekampagne (→ Aufgabe 3.2)
- Eine unzumutbare Belästigung durch eine Werbung via E-Mail liegt vor, wenn keine ausdrückliche Einwilligung des Empfängers vorliegt (§ 7 Abs. 2 Nr. 3 UWG) und/oder die Identität des Absenders verheimlicht oder verschleiert wird (§ 7 Abs. 2 Nr. 4 UWG)
  → Aus Newsletter müssen die erforderlichen Angaben zum Verantwortlichen hervorgehen
  → Newsletter erfordert Einwilligungserklärung unter Einhaltung von Art. 7 EU-DSGVO, zumal kein enger Zusammenhang mit Bestellhistorie bestehen muss

3.4 Newsletter (3)

Telemedienrechtliche Anforderungen:

- Newsletter wird via E-Mail versandt
  → E-Mail ist telemedienrechtlicher Dienst
- Aufgrund von § 12 Abs. 1 TMG muss die Speicherung der Nutzerdaten für den Newsletter auf einer Rechtsvorschrift beruhen, die sich ausdrücklich auf Telemedien bezieht
  → Art. 6 Abs. 1 lit. f EU-DSGVO alleine nicht ausreichend, da kein ausdrücklicher Bezug auf Telemedien
- Telemediendiensteanbieter darf personenbezogene Daten nur zu Zwecken verwenden, die telemedienrechtlich vorgeschrieben bzw. gestattet sind ODER zu denen die Nutzer eingewilligt haben (§ 12 Abs. 2 TMG)
  → Da TMG keine Gestattung zugunsten von Werbung kennt, ist das Vorliegen einer Einwilligungserklärung des Nutzer nötig!

3.4 Newsletter (4)

Telemedienrechtliche Anforderungen: Fortsetzung

- Für den Bezug eines Newsletters muss der Nutzer seine Einwilligung unter Beachtung von § 13 Abs. 3 TMG erteilen
  → Nutzer ist über sein Widerrufsrecht zu informieren!
- Einwilligungserklärung kann auch elektronisch erfolgen, wobei dann § 13 Abs. 2 TMG zu beachten ist:
  ° bewusste & eindeutige Erklärung des Nutzers
  ° Protokollierung der Einwilligungserklärung
  ° jederzeitige Abrufbarkeit der Einwilligungserklärung für Nutzer
  ° Umsetzung zum Widerrufsrecht
- Versand von Newslettern ist in der Datenschutzerklärung aufzuführen (§ 13 Abs. 1 TMG)
- Für den Abruf des Newsletters sind geeignete technische und organisatorische Maßnahmen zu ergreifen (§ 13 Abs. 4 TMG)

3.4 Newsletter (5)

Telemedienrechtliche Anforderungen: Fortsetzung

- *Anmerkung: Am 26.04.2018 hat die Datenschutzkonferenz (= Konferenz der Aufsichtsbehörden) in einem Positionspapier die Ansicht vertreten, dass der 4. Abschnitt des TMG am 25.05.2018 ersatzlos entfallen würde und entsprechende Regeln erst durch Inkrafttreten der ePrivacy-Verordnung wieder gelten würden (vgl. https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf)*
- *Diese Position ist eine Auslegungshilfe, aber noch keine rechtsverbindliche Festlegung. Zudem bezieht sich die Position nur auf Tracking, wofür eine Einwilligung als erforderlich angesehen wird → gleiches dürfte für Newsletter gelten*

3.4 Newsletter (6)

Zur **Einwilligung** für Werbezwecke:

- Aus der Einwilligung muss für den Betroffenen ersichtlich sein, auf was genau sich die Werbung beziehen wird (z.B. durch präzisen Hinweis auf das bestehende Warensortiment bzw. den angebotenen Dienstleistungen; Beschluss LG Berlin vom 09.08.2011; Az. 15 O 762/04)
- Eine Einwilligungserklärung kann auch konkludent erfolgen: Trägt ein Betroffener in einem als freiwillig gekennzeichneten Textfeld unter dortiger Angabe des vorgesehenen Verwendungszwecks seine E-Mail-Adresse ein, darf diese E-Mail-Adresse auch gemäß dem beschriebenen Zweck verwendet werden (Beschluss BGH vom 14.04.2011; Az.: I ZR 38/10)
- Wurde dem Kunden oder Interessenten ab dem Zeitpunkt der Erteilung seiner Einwilligung zu Werbezwecken noch keine Werbung per E-Mail zugesandt, erlischt dessen Einwilligung für Werbe-E-Mails nach 1,5 Jahren (Urteil LG München I vom 08.04.2010; Az.: 17 HK O 138/10)

3.5 Löschkonzept

Aufgabe:

- Entwerfen Sie ein Löschungskonzept zum Newsletterverfahren! Berücksichtigen Sie dabei auch, wie mit Einwilligungen, die nicht für den Newsletterversand genutzt wurden, und mit Datensicherungen umzugehen ist.

3.5 Löschkonzept (1)

- Die Speicherbegrenzung aus Art. 5 Abs. 1 lit. e EU-DSGVO bezieht sich auf Identifizierungsdaten
- Nach Art. 17 Abs. 1 lit. a EU-DSGVO sind personenbezogene Daten zu löschen, wenn sie für die festgelegten Zwecke nicht mehr notwendig sind (oder für rechtliche Verpflichtungen wie z.B. handelsrechtliche Aufbewahrungsfristen nach Art. 17 Abs. 1 lit. e EU-DSGVO bzw. Art. 17 Abs. 3 lit. b oder e EU-DSGVO)
- Nach Art. 30 Abs. 1 lit. f EU-DSGVO sind im Verzeichnis von Verarbeitungstätigkeiten die Regellöschungsfristen festzuhalten
- In der Musterlösung zu Aufgabe 2.2 wurde angegeben für Newsletterverfahren:
  6 Jahre (Geschäftsbriefe)
  1,5 Jahre für Einwilligungen ohne Newsletterversand

3.5 Löschkonzept (2)

- Datensicherung = Maßnahme im Sinne von Art. 32 Abs. 1 lit. b und c EU-DSGVO i.V.m. Art. 6 Abs. 1 lit. f EU-DSGVO
- Für Datensicherungen gelten diese Fristen analog, doch müssen Daten nicht gesondert von Datensicherungsmedien entfernt werden (aus technischen Gründen schwerlich möglich); hier bestimmt sich die Aufbewahrungsfrist nach der längstnötigen Frist des Mediums, wobei diese allerdings nicht künstlich erhöht werden darf, indem unnötig Daten hinzugespeichert werden, die eine deutlich längere Aufbewahrungsfrist benötigen (würde sonst dem Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a EU-DSGVO und andererseits der Datenminimierung nach Art. 5 Abs. 1 lit. c EU-DSGVO widersprechen)

3.5 Löschkonzept (3)

- Newsletterdaten werden entweder in einem eigenen Tool oder im CRM gespeichert
  → Datensicherung kann sich längstens auch nur auf die Aufbewahrungsfrist für (elektronische) Geschäftsbriefe erstrecken (→ 6 Jahre)
  → Datensicherungsdaten soweit aber eigene Datenkategorie
- Die EU-DSGVO bestimmt jedoch nicht exakt, was unter „Löschen“ zu verstehen ist
- Nach ErwG 39 muss sichergestellt sein, dass Unbefugte keinen Zugang zu den Daten haben und diese Daten auch nicht nutzen können
  → reiner Leserechteentzug nicht ausreichend
  → Pseudonymisierung dagegen u.U. schon

3.5 Löschkonzept (4)

- **Produktivdaten aus System entweder unwiederbringlich zu entfernen, zu pseudonymisieren oder zu verschlüsseln** (Zuordnungsmerkmale bzw. Schlüssel dann mit geeignetem Zugriffsschutz zu versehen)
- Nach § 35 Abs. 1 BDSG 2018 ist (auf Basis von Art. 23 Abs. 1 lit. j EU-DSGVO) für eine Datensicherung die Einschränkung (= Sperrung) der Datensicherungsdaten ausreichend, da hierfür (im Gegensatz zu den Produktivdaten) das Interesse des Betroffenen an der Löschung als gering anzusehen ist und eine Löschung wegen der besonderen Art der Speicherung nur mit unverhältnismäßig hohem Aufwand möglich wäre (sequentielles Umkopieren auf ein anderes Datensicherungsmedium mit dem zusätzlichen Risiko, dass durch Umkopieren ggf. die weiter aufzubewahrenden Daten nicht mehr lesbar sind)