5. Übungsblatt zum 17. Juni 2019 zu "Grundlagen des Datenschutzes und der IT-Sicherheit":

Lesen Sie die EU-Datenschutzgrundverordnung (nur Art. 1 – 50 und 77 – 91), das Telemediengesetz (TMG) und das Gesetz gegen den unlauteren Wettbewerb (UWG) durch und beantworten Sie folgende Aufgaben:

5.1 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.

5.2 Ein Unternehmen betreibt hinsichtlich des Umgangs mit Kundendaten folgende technischen Systeme: Web-Portal zur Erhebung von Bestell-wünschen, ERP-System zur Verwaltung der Finanzströme sowie 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!

5.3 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 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 nachstehender 3x3-**Risk-Map**. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

Wahrscheinlichkeit			
3			**Handeln!**
2		**Prüfen!**	
1	**Passt!**		
Schaden	**1**	**2**	**3**

Die jeweiligen Angaben bedeuten dabei Folgendes:

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/Meldepflicht)

5.4 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!

5.5 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)
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*

Allgemeine Hinweise zur Übung:
Die Übung zur LV erfolgt in Form einer Präsenzübung. Für den Notenbonus werden mind. 50 % der max. möglichen Votierpunkte und das Präsentieren von voraussichtlich 3 Lösungen benötigt (abhängig vom Beteiligungsgrad). Jede Aufgabe auf einem Übungsblatt erbringt gleich viele Punkte. **Es gibt verm. 10 Übungsblätter**.
Für das Votieren gilt folgende Regelung:

- Kann die Aufgabenlösung präsentiert werden → voller Punkt
- Existiert für die Aufgabenlösung nur eine Lösungsidee → halber Punkt
- Teilaufgaben werden anteilig gerechnet (d.h. A- bzw. B-Teil jeweils hälftig → insoweit zählt eine Lösungsidee z.B. für den A-Teil nur als ¼-Punkt)
- Zur Lösungspräsentation darf das eigene Lösungsblatt verwendet werden.

Die Einstufung erfolgt durch den Eintragenden und ist entsprechend in die zu Beginn der Übung ausgeteilte Liste einzutragen. Aufgaben, die bereits präsentiert wurden, sind nachträglich nicht mehr votierbar.
Wer Votierpunkte angegeben hat, kann vom Dozenten zur Präsentation seiner Lösung bzw. Lösungsidee aufgerufen werden. Nachweisbar unkorrektes Votieren wird mit 0 Punkten für das gesamte Übungsblatt gewertet.

Gutes Gelingen!