3. Übungsblatt zum 2. Juni 2025 zu den "Grundlagen des Datenschutzes und der IT-Sicherheit":

Lesen Sie neben der EU-Datenschutzgrundverordnung auch Art. 3, 5 & 50 der KI-VO durch (elektronisch abrufbar unter: https://www.uni-ulm.de/?id=36570) und beantworten Sie folgende Aufgaben:

3.1 Leiten Sie aus den vier **ethischen Grundsätzen** aus der EU-Leitlinie für eine vertrauenswürdige KI als auch aus der KI-VO **handlungsrelevante Vorgaben** für die **Gestaltung eines** (Nicht-Hochrisiko-)**KI-Systems** ab!

3.2 Welche Vorschriften aus der EU-DSGVO würden derzeit bei der **Zulässigkeitsprüfung von KI-Systemen** mit welchem Ergebnis herangezogen werden?

3.3 Für ein **KI-System** wurde Folgendes geplant:

- Das KI-System speichert neben der Cookie-ID alle vom Nutzer eingegebenen personenbezogenen Daten zu den gestellten Aufgaben hinzu, um künftige Anfragen vom gleichen Nutzer personalisieren zu können (z.B. durch persönliche Ansprache).
- Anhand der Themen gestellter Fragen, wird für den Nutzer eine geeignete Werbung auf der Webseite eingebunden, auf der das KI-System genutzt werden kann.
- Als Trainingsdaten für das KI-System wurden Daten verwendet, die von den Systemerstellern anhand geplanter Einsatzzwecke im Hinblick auf Funktionalität erstellt worden sind.
- Antworten des KI-Systems werden von dem Nutzer ob ihrer Nützlichkeit bewertet und diese Bewertung fließt als zusätzliche Trainingsdaten ein.
- Das KI-System soll als Public Cloud implementiert werden, damit es weltweit und jederzeit genutzt werden kann.

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 Abhilfemaßnahme 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)

3.4 Welche **technischen Maßnahmen** sollten für ein **KI-System** zum maschinellen Lernen implementiert werden (sowohl bei dessen Entwicklung als auch beim Betrieb), damit es widerstandsfähig gegenüber Fehlern, Störungen oder Unstimmigkeiten (inkl. aus Rückkopplungsschleifen) ist?

3.5 Eine **kritische Infrastruktur** muss **Protokolldaten** in sein **System zur Angriffserkennung** einspeisen. Skizzieren Sie hierzu Beachtenswertes aus dem Datenschutz unter Berücksichtigung der Vorschriften aus dem BSIG für kritische Infrastrukturen!
Hinweis: Von den Vorschriften aus dem BSIG sind aufgabenrelevant:

§ 2 Begriffsbestimmungen

(8) Protokolldaten im Sinne dieses Gesetzes sind Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten.

(9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.

§ 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

(2) Protokolldaten […] dürfen […] längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts […] zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1a) Die Verpflichtung […], angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst […] auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

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. 6 Übungsblätter**.

Für das Votieren gilt folgende Regelung:

- Kann die Aufgabenlösung präsentiert werden [P] → voller Punkt
- Existiert für die Aufgabenlösung nur eine Lösungsidee [I] → 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)

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!