# Lösungen

# Übungsklausur

## Vorlesungen des ULD an der CAU Kiel
## Datenschutz: Recht und Technik

Ansprechperson / Koordination:
Henry Krasemann
Email: uld7@datenschutzzentrum.de
Tel.: 0431-9881398

**I. Einführung in das allgemeine Datenschutzrecht**

1) Warum stellt das Recht auf informationelle Selbstbestimmung eine fundamentale Voraussetzung für eine moderne Demokratie dar? (4 Punkte)

*Lösung: Verhinderung eines Anpassungs- bzw. Rechtfertigungsdrucks aufgrund von Angst vor Sanktionen, Erhalt der Teilnahmemöglichkeit am politischen Willensbidlungsprozess für den einzelnen Bürger.*

2) Nennen Sie drei Aspekte die das Recht auf informationelle Selbstbestimmung ausmachen und erläutern diese mit jeweils einem Satz. (3 Punkte)

*Lösung: Selbstbestimmung: freie eigene Entscheidung*
*Erforderlichkeitsgrundsatz: Datenverarbeitung nur soweit zur Zweckerrechung notwendig*
*Gesetzesvorbehalt: Eingriff in die Selbstbestimmung nur aufgrund eines Gesetzes*

3) Welche Aussagen treffen zu (2 Punkte):

a.) Das Bundesdatenschutzgesetz ist für Bundesbehörden anwendbar.
b.) Das Bundesdatenschutzgesetz ist in Bezug auf den Datenschutz gegenüber dem Telekommunikationsgesetz vorrangig anwendbar.
c.) Im Bundesdatenschutzgesetz wird die Datenverarbeitung von Daten juristischer Personen geregelt.
d.) Das Bundesdatenschutzgesetz ist nicht anwendbar, wenn die Datenverarbeitung ausschließlich für persönlich familiäre Tätigkeiten erfolgt.

*Lösung: a und d*

4) Unter welchen Umständen ist eine Datenverarbeitung nach dem Bundesdatenschutzgesetz rechtmäßig? (2 Punkte)

*Lösung: Entweder Einwilligung, BDSG oder andere Rechtsvorschrift § 4a BDSG*

5) Nennen Sie drei Voraussetzungen einer wirksamen Einwilligung nach § 4a BDSG (2 Punkte)

*Lösung: Information, Schriftform, Freiwilligkeit*

## II. Datenschutz und Technik

1) „Diese Nachricht zerstört sich in 5 Sekunden selbst." – Welches **Schutzziel** soll mit dem in diesem Satz beschriebenen Mechanismus erreicht werden? (1 Antwort, 1 Punkt)

   a) Vertraulichkeit
   b) Verfügbarkeit
   c) Integrität

*Lösung: a)*

2) Bei einem der in der vorherigen Aufgabe aufgeführten Schutzziele spricht man davon, dass die **Auswirkungen einer Schutzzielverletzung in jedem Fall irreversibel** (also unumkehrbar) sind. Um welches Schutzziel handelt es sich und warum? (1 Antwort, 1 Punkt)

*Lösung: Es handelt sich um das Schutzziel „Vertraulichkeit". Eine Verletzung des Schutzziels „Vertraulichkeit" bedeutet, dass jemand unberechtigt Kenntnis von Daten erlangt hat. Dies kann nicht ungeschehen gemacht werden.*

3) Wie kann man feststellen, ob das **Schutzziel „Integrität" verletzt** wurde? Nennen Sie ein Beispiel! (1-2 Sätze, 2 Punkte)

*Lösung: Eine Verletzung der Integrität von Daten kann beispielsweise erkannt werden, wenn für den integren Original-Datenbestand Hashwerte oder digitale Signaturen verwendet wurden. Werden auf dem neuen Datenbestand erneut Hashwerte oder digitale Signaturen nach demselben Verfahren gebildet und weichen diese von den Werten für den Original-Datenbestand ab, liegt eine Verletzung der Integrität vor.*

4) Welche der folgenden speziellen **Anforderungen** für eine technisch-organisatorische Umsetzung werden explizit im **Bundesdatenschutzgesetz** (BDSG) aufgeführt? (2 Antworten, 2 Punkte)

   a) Inhaltskontrolle
   b) Fahrscheinkontrolle
   c) Weitergabekontrolle
   d) Personen-Statuskontrolle
   e) Zugriffskontrolle
   f) Datenvermeidungskontrolle

*Lösung: c) und e)*

5) Skizzieren Sie das **Spannungsfeld** zwischen **wirtschaftlichen und technischen Anforderungen an IT-Systeme** auf der einen Seite und **Datenschutz** auf der anderen

Seite durch Ankreuzen der folgenden Gegenüberstellung! (Eine Doppeltnennung, 2 Punkte)

| wirtschaftliche / technische Anforderung | | Datenschutz-anforderung |
|---|---|---|
| ☒ | Gewinnmaximierung | |
| ☐ | Transparenz der Datenverarbeitung für die Betroffenen | ☒ |
| ☒ | umfassender Zugriff auf alle Informationen | |
| ☒ | Redundanzvermeidung | |
| | Recht auf informationelle Selbstbestimmung | ☒ |
| | Rechte der Betroffenen | ☒ |
| ☒ | Vermeidung von Single Points of Failure | |

6) Sie sind IT-Sicherheitsbeauftragte(r). Ihr Unternehmen erstellt und vertreibt **Soft- und Hardware für Verschlüsselungsverfahren**. Sie werden gebeten, einen passenden internationalen Sicherheitsstandard auszuwählen, an dem sich Ihr Unternehmen bei der **Organisation der internen Sicherheit** (also der Entwicklungs-, Herstellungs- und Vertriebsprozesse) orientieren soll und dessen Einhaltung **zertifiziert** werden soll. Ihre Kollegen aus der Entwicklungsabteilung schlagen die **Norm ISO/IEC 17799/ISO 27002** vor.

   Wenn dies ein guter Vorschlag ist: Schreiben Sie eine zustimmende Begründung!

   Wenn dies ein schlechter Vorschlag ist: Begründen Sie Ihre Ablehnung, nennen Sie eine Alternative und begründen Sie sie! (3 Punkte)

*Lösung: Die Norm ISO/IEC 27002 enthält Best-Practice-Ansätze für die unternehmensweite Organisation von IT-Sicherheit (IT-Sicherheitsmanagement) und die Realisierung von IT-Sicherheitsmaßnahmen. Diese bieten zwar gute* **Hinweise** *zur Umsetzung der Sicherheits-maßnahmen, aber keinen* **zertifizierbaren** *Prozess für die Auswahl und die Überprüfung der Umsetzung. Hierfür wäre die Norm ISO/IEC 27001 geeignet, gegen die eine Zertifizierung erfolgen kann.*

7) Bei der **Einrichtung eines Information Security Management Systems (ISMS)**, z.B. nach ISO 27001, sind verschiedene Aufgaben zu erledigen. Bringen Sie sie in die Reihenfolge (Nummern von 1 bis 6 vergeben)! (3 Punkte; je ½ Punkt)

_4__ Sicherheitsmaßnahmen festlegen

_3__ Risikobewertung vornehmen

_1__ Grenzen und Umfang des ISMS festlegen

_2__ Risikoanalyse- und -bewertungsmethode festlegen

_6__ Zutrittskontrollmaßnahmen implementieren

_5__ ausgewählte Sicherheitsmaßnahmen dokumentieren

8) Ein Verein möchte seinen Mitgliedern für alle Arten der Wahlen und Mitgliederbeteiligungen ein Online-Forum anbieten, in dem Mitglieder ihr Votum zu bestimmten Fragen abgeben können. Ein Online-Forum wirbt für sich wie folgt:

*„Wir setzen auf maximale Transparenz: Jedes abgegebene Votum ist unmittelbar für alle Mitglieder sichtbar. Damit sieht jeder nach Abgabe seiner Stimme sofort, dass sie korrekt gezählt wird – eine Manipulation ist also ausgeschlossen. Eine Überprüfung der korrekten Stimmenzählung ist selbst noch Jahrzehnte später möglich, denn wir haben das Forum so gebaut, dass Daten nie gelöscht werden."*

Angenommen, diese Aussagen stimmen. Welche der folgenden Aussagen sind korrekt, wenn man **Kriterien für datenschutzfördernde Technik** anlegt? (3 Antworten, 3 Punkte)

a) Für eine umfassende Bewertung des Online-Forums fehlen beispielsweise Aussagen zur Aufklärung der Betroffenen über die Verarbeitung ihrer personenbezogenen Daten und zur Sicherheit der Datenverarbeitung.
b) Die maximale Transparenz ist zu begrüßen. Nur wenn alle Mitglieder immer ihre eigenen Voten und die von anderen sehen können, ist eine datenschutzfördernde Realisierung möglich.
c) Dass die Voten für alle Mitglieder über Jahrzehnte sichtbar sind und kein Löschen vorgesehen ist, verstößt gegen das Prinzip der Datensparsamkeit.
d) Unter „Transparenz für den Betroffenen" in Hinblick auf die Voten ist nicht zu verstehen, dass alle die eigenen Voten sehen können, sondern dass für jeden nur seine eigenen Voten transparent sind.
e) Es ist zu begrüßen, dass die Daten noch nach Jahrzehnten verfügbar sind. Dies ist wichtig für die Qualitätssicherung.

*Lösung: a), c) und d)*

**III. Kundendatenschutzrecht**

1. Stellen Sie sich vor

a) Sie kommen zum Bäcker und wollen Brötchen kaufen.

b) Sie bestellen bei einem Online-Buchhändler das Buch Wirtschaftsinformatik 1.

Ist es datenschutzrechtlich zulässig, wenn Sie dabei nach Ihrem Namen und Ihrer Adresse gefragt und diese Informationen abgespeichert werden? Bitte erläutern Sie Ihre Antwort. (3 Punkte)

*Lösung: Die Zulässigkeit der Datenverarbeitung bestimmt sich nach dem Vertragszweck. Ist es für die Erfüllung des Vertragszwecks erforderlich bestimmte Daten zu erheben und zu speichern, so ist die Erhebung und Speicherung dieser Daten zulässig.*

*a) Zweck des Brötchenkaufs ist die reine Abwicklung eines Direktgeschäfts. Die Brötchen und das Geld sollen direkt im Laden übergeben werden. Für die Erfüllung dieses Geschäfts ist es nicht erforderlich, Name und Adresse zu erheben und zu speichern.*

*b) Zweck der Online-Bestellung ist die Abwicklung eines Distanzgeschäfts. Das Buch kann nicht unmittelbar übergeben sondern muss versendet werden. Für die Versendung ist es erforderlich, den Namen und die Adresse des Kunden zu kennen. Daher ist es datenschutzrechtlich zulässig, diese Daten für die Vertragsabwicklung zu erheben und zu speichern*.

2. Sie stehen in einer langen Schlange an einer Supermarktkasse. Sie sind an der Reihe und zahlen mit EC-Karte. Die Kassiererin fragt Sie, ob Sie damit einverstanden sind, dass in Zukunft alle Ihre Einkäufe mit EC-Karte registriert werden. Wenn Sie nicht zustimmen, sei in Zukunft eine Zahlung mit EC-Karte für Sie nicht mehr möglich.

Sie stimmen zu. Die Kassiererin notiert sich Ihren Namen sowie Ihre Kontonummer. Die Supermarktkette wertet bei all Ihren zukünftigen Einkäufen mit EC-Karte Ihr Kaufverhalten aus (Beträge, Produkte, Filialen, Datum, Uhrzeiten), um das Angebot darauf abzustimmen.

Haben Sie an der Kasse eine wirksame Einwilligung in die Erhebung, Verarbeitung und Nutzung Ihrer Daten abgegeben? Bitte erläutern Sie Ihre Antwort. (3 Punkte)

*Lösung: Nein, es liegt keine wirksame Einwilligung nach § 4a BDSG vor.*
*Es bestehen Zweifel an der Freiwilligkeit, weil negative Konsequenzen für den Fall der Ablehnung drohen.*
*Es wurden nicht die konkreten Zwecke der Erhebung, Verarbeitung und Nutzung Ihrer Daten dargelegt.*
*Die Erklärung wurde nicht in Schriftform abgegeben.*

## IV. Arbeitnehmerdatenschutzrecht

1. Worin liegt die Problematik der Einwilligung des Arbeitnehmers in die Datenerhebung, -verarbeitung und -speicherung im Arbeitsverhältnis? (6 Punkte)

*Lösung:*
*- Freiwilligkeit der Einwilligung im Arbeitsverhältnis problematisch*
*- Entscheidungsfreiheit durch existentielle Bedeutung des Arbeitsverhältnisses faktisch eingeschränkt*
*- Einwilligung darf nicht durch wirtschaftliche Machtposition „abgepresst" werden*

*Fazit: Einwilligung geht in der Regel nur, wenn DV mit dem Arbeitsverhältnis nichts zu tun hat, d. h. AN bei Verweigerung der Einwilligung keine Nachteile befürchten muss.*

## V. Datenverarbeitung zur Strafverfolgung und Gefahrenabwehr (Befugnisse der Sicherheitsbehörden, Mitwirkungspflichten)

1. Im Gefahrenabwehr- und Strafverfolgungsrecht gibt es allgemeine und spezielle Befugnisnormen, die die Datenverarbeitung erlauben. Welche Aussagen sind richtig? (2 Antworten richtig – 3 Punkte)

a) Die speziellen Befugnisnormen gelten vorrangig vor den allgemeinen Befugnisnormen.

b) Liegen die speziellen Voraussetzungen für eine Telefonüberwachung nicht vor, kann sie nur durchgeführt werden, wenn die Voraussetzungen der allgemeinen Befugnisnorm erfüllt sind.

c) Gibt es für eine Maßnahme, die einen schwerwiegenden Grundrechtseingriff darstellt (z.B. Online-Durchsuchung), keine spezielle Befugnis, die diese erlaubt, ist sie unzulässig. Auch wenn die Voraussetzungen der allgemeinen Befugnis erfüllt sind, kann die Maßnahme hierauf nicht gestützt werden.

*Lösung: a) und c)*

2. Welche Grundsätze müssen Gefahrenabwehr- und Strafverfolgungsbehörden beachten, wenn sie verdeckte Ermittlungsmaßnahmen durchführen? (2 Antworten richtig – 3 Punkte)

a) Sie müssen die Einwilligung des Betroffenen einholen.

b) Sie müssen sicherstellen, dass keine Daten aus dem Kernbereich privater Lebensgestaltung erhoben und gespeichert werden.

c) Sie müssen sicherstellen, dass Dritte von dieser Maßnahme nicht betroffen werden.

d) Sie müssen den Betroffenen grundsätzlich nach Abschluss der Maßnahme benachrichtigen.

*Lösung: b) und d)*

## VI. Datenschutz in Telemedien / Sozialen Netzwerken

1. Nennen Sie zwei datenschutzrechtliche Problembereiche bei sozialen Netzwerken (2 Punkte)

*Lösung: z. B. Einwilligung von Jugendlichen / Kindern, Recht am eigenen Bild, mangelhafte Information, kein Überblick über Veröffentlichung der Daten, Veröffentlichung von Daten Dritter, Kontaktabgleich etc…*

2. Sie laden ein Partyfoto von sich und einem Freund in ein soziales Netzwerk, wobei dieses von allen Nutzern des Netzwerkes gesehen werden kann. Was müssen Sie beachten? (2 Punkte)

*Lösung: Einwilligung des Freundes notwendig.*

3. Nennen Sie zwei Gesetze (neben dem BDSG), die bei Sozialen Netzwerken bzgl. Datenschutz anwendbar sein können. (2 Punkte)

*Lösung: Telekommunikationsgesetz, Telemediengesetz*

**VII. Datenschutz in mobilen Endgeräten**

1. Beschreiben Sie, warum Datenschutz in mobilen Endgeräten so wichtig ist. (1 Punkt)

*Lösung: Mobile Endgeräte sind immer beim Nutzer und geben detailliert Auskunft über dessen Persönlichkeit, sie zeichnen verstärkt auch biometrische Daten auf und sind mehr und mehr gleichzusetzen mit dem Zugang zu sozialen Netzwerken. Mobile Endgeräte werden zum mobilen Speicher für alle relevanten Bereich des Alltags. Sie sind aufgrund Ihrer Mobilität schwerer zu schützen und schneller fremdem Zugriff ausgesetzt.*

2. Beschreiben Sie das Datenschutz-Schutzziel Vertraulichkeit und Integrität und welche Aspekte mobiler Betriebssysteme dabei eine Rolle spielen. (jeweils 2 Punkte)

*Lösung:*

*a) Vertraulichkeit bezeichnet den gesicherten Nichtzugriff auf Informationen. Bei mobilen Betriebssystemen ist insbesondere eine zuverlässige und nutzerfreundliche Verschlüsselung relevant.*

*b) Integrität bezeichnet die gesicherte Echtheit von Informationen. Bei mobilen Betriebssystemen ist insbesondere Malware relevant.*

3. Sie sind Entwickler und sollen ein App für Online-Banking schreiben. Welche technischen Maßnahmen halten Sie auf der Anwendungsebene für sinnvoll? (1 Punkt)

*Lösung: Bei einer Online-Banking App wäre etwa sicherzustellen, dass Zugangsdaten auf dem Gerät sicher verschlüsselt sind. Sinnvoll wäre auch Zugangsgerät (Gerät auf dem die App läuft) und Identifikationsgerät (Gerät, dass zum Beispiel die mobile TAN erhält) nicht identisch sind. Eindeutige Gerätenummern sollten nicht als Identifikator genutzt werden.*

**VIII. Betrieblicher Datenschutz und Auftragsdatenverarbeitung**

1. Ein Autohändler möchte die Datenhaltung redundant ausgestalten und hierzu auch die Kundendatenbank im Rechenzentrum eines lokalen Drittanbieters spiegeln lassen

a) Über welche rechtliche Gestaltung ließe sich dies im Einklang mit dem BDSG gestalten? (½ Punkt) Norm? (½ Punkt)

*Lösung: Auftragsdatenverarbeitung, § 11 BDSG*

b) Welche Pflichten muss das Rechenzentrum dabei beachten? (1 Punkt).

*Lösung: siehe Pflichten des Auftragnehmers in § 11 Abs. 3 BDSG*

c) Bedarf die geplante Übermittlung an das Rechenzentrum einer Einwilligung der Kunden? Nennen sie die Norm bzw. die Normen, auf die Sie Ihre Antwort stützen. (2 Punkte)

*Lösung: Nein. Sind die Voraussetzungen einer Auftragsdatenverarbeitung gegeben ist Rechenzentrum kein Dritter mehr (§ 3 VIII S. 3 BDSG). Dann fehlt es auch an einer Übermittlung (§ 3 IV Nr. 3 BDSG).*

2. Welche wesentliche Verbesserung für den Status von betrieblichen Datenschutzbeauftragten hat die BDSG-Novelle 2009 herbeigeführt? (1 Punkt)

*Lösung: Kündigungsschutz*