Prof. Dr. Viola Schmid LL.M.

Informations- und Datenschutzrecht

Abschlussklausur WS 2004/2005

01.02.2005

Name:	**Vorname:**
Studiengang:	**Matrikelnummer:**

Teil I – 20 %

1. Was versteht die Vorlesung unter „Organisation“ von Daten? (4 Punkte)
Unter Organisation von Daten versteht die Vorlesung die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Unter Erhebung ist dabei das Beschaffen der Daten zu verstehen, unter Verarbeiten das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Nutzung ist jede Verwertung personenbezogener Daten, sofern es sich nicht um Verarbeitung handelt (vgl. Art. 3 Abs. 2-5 BDSG).

2. Was ist der Normzweck von § 86a VwGO? (4 Punkte)
Der Normzweck von § 86a VwGO ist die Möglichkeit, verwaltungsgerichtliche Prozesshandlungen via e-mail durchführen zu können. Dabei geht es um das Einreichen von elektronischen Dokumenten bei Gericht sowie um die Zustellung von Seiten des Gerichts. Voraussetzung ist, dass das Format der Daten für die Bearbeitung des Gerichts geeignet ist (vgl. § 86a Abs. 1 VwGO).

3. Was versteht man unter der FÖR-TUD-Formel I^3A? (4 Punkte)
Unter I³A versteht man die 4 Sicherheitsschutzziele Identität, Integrität, Intimität (Informationsvertraulichkeit) und Authentizität. Diese 4 Schutzziele sollen die Verfügbarkeit und die Verbindlichkeit gewährleisten. I³A ist nicht im Recht verankert, sondern aus einertechnikwissenschaftlichen Perspektive entwickelt worden (vgl. IT-Sicherheit, Claudia Eckert). Die Sicherheitsziele sind Voraussetzung für die Sicherheit von IT-Systemen und insbesondere Signaturen.

4. Beschreiben Sie das Verhältnis von Sicherheit, IT-Sicherheit und Datenschutz! (8 Punkte)
Weder der Begriff „Sicherheit" noch der Begriff „IT-Sicherheit" ist gesetzlich legal normübergreifend definiert. Insbesondere der Begriff „IT-Sicherheit" ist normspezifisch zu entwickeln und verlangt die Einbeziehung der technikwissenschaftlichen Perspektiven (vgl. 3). Das Verhältnis zwischen IT-Sicherheit und Sicherheit ist exemplarisch in Art. 29 EU verdeutlicht: Die EU möchte die Sicherheit erhöhen. Das setzt Wissen voraus, insbesondere bei der präventiven Straftatenbekämpfung. Daher will die EU IT-Systeme nutzen um Wissen zu mehren und zu verbreiten. Dabei geht es um länderübergreifende Behörden (z.B. EUROPOL) aber auch die Interoperabilität der mit mitgliedsstaatlichen Systemen. Diese Systeme müssen selbst sicher sein, es kann durch den Einsatz solcher Systeme keine Sicherheit ohne IT-Sicherheit geben (vgl. Art. 29 Abs. 1 Lit. a) EU).
Das Verhältnis von Sicherheit bzw. IT-Sicherheit und Datenschutz ist akzessorisch. Es kann keinen Datenschutz ohne Datensicherheit geben. Die Datensicherheit bzw. IT-Sicherheit ist daher als wesentliches Instrument des Datenschutzes anzusehen.

Anmerkung FÖR: Hier hätten weitere Normen zum IT-Sicherheitsrecht /Datenschutzrecht genannt werden können (etwa: § 9 BDSG mit Anlage, OECD-Guidelines „culture of security"). Des weiteren hätte auf mögliche Gefährdungen bei Verletzung der IT-Sicherheit (etwa in Krankenhäusern) hingewiesen können. Insgesamt hätte mehr mit Beispielen gearbeitet werden können.

Teil II: 30%

1. Nennen Sie sechs Auslegungsmethoden! (6 Punkte)
grammatische Auslegung
historische Auslegung
systematische Auslegung
teleologische Auslegung
dogmatische Auslegung]
dynamisch-technische Auslegung
[normenhierarchische Auslegung]

2. a) Welchen Normen im StGB entsprechen Art. 3 und Art. 4 der CCC?
Art. 3 CCC entspricht § 202a StGB
Art. 4 CCC entspricht § 303a StGB

b) Welche Daten dürfen nach Art. 16 CCC gespeichert werden? (6 Punkte)

Art. 16 CCC gewährleistet eine rasche Sicherung von spezifischen Computerdaten, einschließlich Verbindungsdaten, die zuvor bereits durch ein Computersystem gespeichert wurden (vgl. Art. 16 Abs. 1 CCC). Insbesondere gilt dies, wenn es Grund zur Annahme gibt, dass diese Daten leicht verloren gehen oder modifiziert werden könnten (vgl. Art. 16 Abs. 1 CCC).

Anmerkung FÖR: Hier hätte noch auf die Legaldefinition des Art. 1 b, d CCC hingewiesen werden können. Weiterhin fehlt der Hinweis, dass Daten „on the fly" nicht erfasst sind.

3. Nennen Sie „europäische" (auch EMRK) und deutsche Normen zur Meinungsäußerungsfreiheit und zur Informationsfreiheit! (10 Punkte)

Deutsche Normen zur Informationsfreiheit: Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG („Informationelle Selbstbestimmung")

Deutsche Normen zur Meinungsäußerungsfreiheit: Art. 5 GG (Recht der freien Meinungsäußerung)

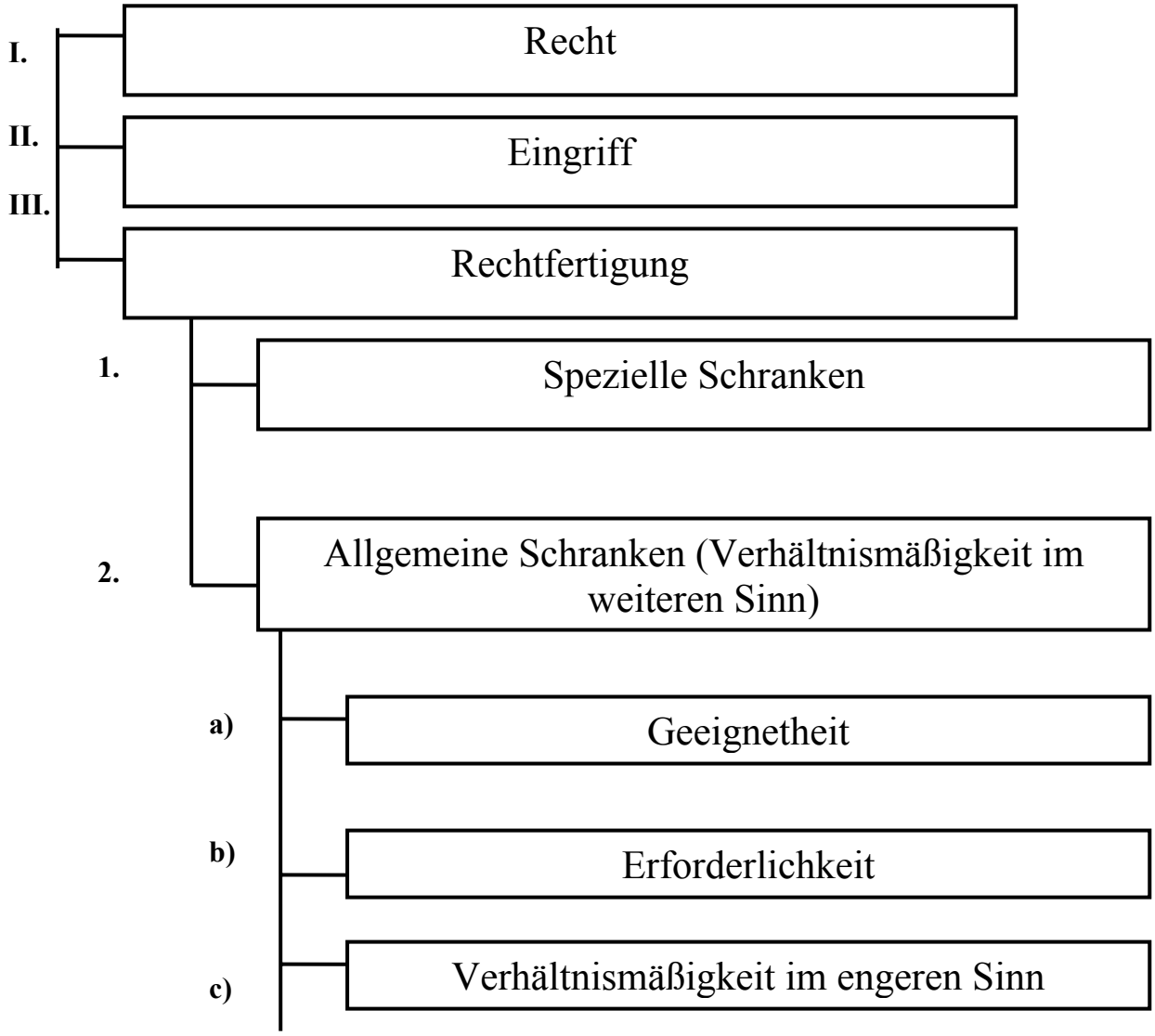
=> für das Land Berlin gibt es das im Cyberlaw abgedruckte Informationsfreiheitsgesetz Berlin

EMRK: Meinungsfreiheit: Art. 10 EMRK
Informationsfreiheit: im weiten Sinne kann hier auch Art. 10 bzw. Art. 11 EMRK angegeben werden.

Europäisches Recht: Art. 11 Grundrechtscharta der EU (Meinung- und Informationsfreiheit) InfZugV, sowie Art. 255 EG-Vertrag, die den Zugang zu elektronischen Dokumenten der EU regeln (Teil der Informationsfreiheit)

Amnerkung FÖR: Hier hätten noch bei entsprechender Erläuterung Normen zur Religionsfreiheit (etwa Art. 4 Abs. 1, 4 GG) genannt werden können, da auch die freie Religionsausübung als Teil der Ausübung der Meinungsfreiheit verstanden kann.

4. Füllen Sie das folgende RER-Prüfungsschema aus (ohne Erläuterung)!: (8 Punkte)



Teil III – 45%

Beantworten Sie die Fragen zum nachstehenden Sachverhalt! (45 P.)

Sachverhalt
Der Datenschutzbeauftragte einer hessischen Universität hat von dem Auskunftsersuchen Kenntnis erhalten und weist nach juristischer Recherche und Lektüre unterschiedlicher Gerichtsentscheidungen auf die Zweifel an der Verfassungsmäßigkeit des Auskunftsverlangens hin. Die Präsidentin der Universität, die Philosophieprofessorin P, sieht sich wie Odysseus zwischen Scylla und Charybdis: Wenn sie dem rechtswidrigen Auskunftsverlangen nachkommt, verletzt sie das Recht auf informationelle Selbstbestimmung des Studenten; wenn sie sich dem rechtmäßigen Auskunftsverlangen widersetzt, verletzt sie geltendes Recht. Sie fragt deshalb den Datenschutzbeauftragten D, wer bei dieser Datenorganisation die Rechtmäßigkeit zu prüfen und zu verantworten habe.

§ 26 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG)
[Besondere Formen des Datenabgleichs]

(1) Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Verhütung von Straftaten erheblicher Bedeutung
1. gegen den Bestand oder die Sicherheit des Bundes oder eines Landes oder
2. bei denen Schäden für Leben, Gesundheit oder Freiheit oder gleichgewichtige Schäden für die Umwelt zu erwarten sind,
die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich und dies auf andere Weise nicht möglich ist. Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

(2) Das Übermittlungsersuchen ist auf Namen, Anschriften, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken. Werden wegen technischer Schwierigkeiten, die mit angemessenem Zeit- oder Kostenaufwand nicht beseitigt werden können, weitere Daten übermittelt, dürfen diese nicht verwertet werden.

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, daß er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten. Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Vernichtung der Unterlagen nach Satz 1 folgt, zu vernichten.

(4) Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.

(5) Personen, gegen die nach Abschluss einer Maßnahme nach Abs. 1 weitere Maßnahmen durchgeführt werden, sind hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zweckes der weiteren Datennutzung erfolgen kann. § 15 Abs. 7 HSOG gilt entsprechend.

1. Erklären Sie die Bedeutung des "Grundsatzes der Amtshilfefestigkeit". (15 Punkte)
Prinzipiell beinhaltet das VwVfG in § 4 die allgemeine Pflicht zur Amtshilfe. Jede Behörde hat einer anderen Behörde auf Ersuchen ergänzend Hilfe zu leisten (§ 4 Abs. 1 VwVfG). Im Falle der Rasterfahndung, die eine spezielle Organisationsmaßnahme von Daten bedeutet, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, das im sog. „Volkszählungsurteil“ des BVerfG (BVerfGE 65, 1) eindeutig aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG entwickelt wurde. Bei einer derartigen Maßnahme gilt, und das hat sich in einer dynamischen Auslegung herauskristallisiert und ist nicht explizit im Recht verankert, der

Grundsatz der Amtshilfefestigkeit. Grundsätzlich hat die ersuchte Behörde in diesem Fall die Universität, also nicht prinzipielle Amtshilfe zu leisten. Doch es handelt sich um einen „Grundsatz“ was die Existenz von Ausnahmen impliziert: Ausnahmen können sein: Einwilligung des Betroffenen oder eine spezielle Vorschrift wie § 26 HSOG. Gerade § 26 HSOG ist nach Auffassung der Vorlesung als Spezialität bzw. spezielles Verwaltungsverfahrensrecht zu sehen. Hier geht es um die präventive Verhütung von Straftaten mit erheblicher Bedeutung (vgl. § 26 Abs. HSOG), so dass der Grundsatz der Amtshilfefestigkeit nicht ohne weiteres gilt. Auch kann sich die Universität aufgrund der Subsidiarität des VwVfG beispielsweise nicht auf § 5 Abs. 3 VwVfG berufen und die Übermittlung grundsätzlich wegen beispielsweise einem unverhältnismäßig großen Aufwand (§ 5 Abs. 3 Nr. 2 VwVfG) unterlassen.
Es gilt das Prinzip der effektiven und effizienten Umsetzung, daher die Spezialität des HSOG gegenüber dem VwVfG und daher damit verbunden die Einschränkung des Grundsatzes auf Amtshilfefestigkeit in diesem Falle.

Anmerkung FÖR: Hier hätten noch Ausführungen zum Gefahrenpotenzial bei unbegrenztem behördlichen Datenaustausch(Stichworte „gläserner Mensch“, „umfassender Datenaustausch“) getroffen werden können. Insgesamt aber eine stringente und überzeugende Darstellung.

2. Welchen Prüfungsumfang geben § 7 Abs. 2 VwVfG und § 14 HDSG für den oben dargestellten Sachverhalt vor? (15 Punkte)

Nach § 7 Abs. 2 VwVfG trägt die ersuchende Behörde die Verantwortung für die Maßnahmen, die ersuchte Behörde ist für die Durchführung verantwortliche. Allerdings wird im Falle der Rasterfahndung das VwVfG keine Anwendung finden, da dieses gem. § 1 VwVfG nur für Länder gilt, wenn sie Bundesrecht ausführen. Wie in der Vorlesung dargestellt ist hier also das hessische Verwaltungsverfahrensgesetz hinzuzuziehen, das leider nicht im Cyberlaw abgedruckt ist. Bezüglich des HDSG ist das HVwVfG allerdings wiederum als grundsätzlich subsidiär anzusehen. Es gelten somit bezüglich des Prüfungsumfangs und der Verantwortlichkeit die Regeln, die im HDSG stehen (im HSOG, das noch spezieller ist, gibt es für die Verantwortlichkeit eine Norm, die aber anderes aussagt als § 14 HDSG, daher gibt es § 14 HDSG).
Gem. § 14 HDSG tragen sowohl Empfänger als auch übermittelnde Stelle (Uni) in diesem Fall die Verantwortung (vgl. § 14 S. 2 HDSG).
Bezüglich des Prüfungsumfangs gibt es für die Universität zwei Möglichkeiten: Entweder sie geht von der Schlüssigkeit der Anfrage aus (§ 14 S. 3 HDSG) und prüft nicht weiter, oder sie stellt die Schlüssigkeit in Frage. In diesem Fall hat sie die Erforderlichkeit der Organisationsmaßnahmen zu prüfen (vgl. § 14 S. 4 HDSG). Das könnte z.B. im Rahmen einer RER-Prüfung bezogen auf das „Grundrecht“ auf Datenschutz (informationelle Selbstbestimmung) erfolgen. Für die Überprüfung der Schlüssigkeit hat die empfangende Behörde (BKA/LKA) die erforderlichen Angaben zu machen (vgl. § 14 S. 5 HDSG).

Anmerkung FÖR: Hier hätten weitere Erläuterungen zu den Begriffen Zuständigkeit, Schlüssigkeit und Erforderlichkeit (§ 11 HDSG) erfolgen können. Die Subsidiarität des VwVfG hätte mit § 1 Abs. 1 VwVfg dargestellt werden können. Gut wurde die Abgrenzung Landesrecht- Bundesrecht dargestellt (musste für eine gute Lösung aber nicht erkannt werden).

3: Welche Interessen/Sachverhaltskonturen entnehmen Sie dem Fall, so er mit folgendem Schema strukturiert wird? (15 Punkte)

Personal-Aktiv
Personal-passiv Datenschutz
Personal-passiv Informationskosten
Objekt
Kausal/Zweck
Qualität der Informationstechnik
Verfahren
Rechtfertigung/ Verhältnismäßigkeit

Personal-aktiv: Die ermittelnde Behörde (LKA/BKA) ist an personenbezogenen Daten eines Studenten interessiert.
Personal-passiv, Datenschutz: Ein Student arabischer Herkunft ist an der Reservierung und Sicherung seiner von der Universität erhobenen personenbezogenen Daten interessiert.
Personal-passiv, Informationskosten: Die Universität hat mit Kosten für die Aufbereitung und Weitergabe der erhobenen Daten zu rechnen.
Objekt: Personenbezogene Daten (vgl. § 3 Abs. 1 BDSG) eines Studenten arabischer Herkunft
Kausal/Zweck: Die Behörde möchte die Sicherheit erhöhen und terroristische Anschläge verhindern.
Qualität der Informationstechnik: Die Daten werden organisiert (vgl. § 3 Abs. 2 BDSG), automatisiert verarbeitet und an die anfragenden Behörden übermittelt (vgl. § 26 Abs. 1 HDSG). Sie werden dann automatisiert abgeglichen (§ 26 Abs. 1 HDSG).
Verfahren: Entsprechend § 26 Abs. 4 HDSG steht die Maßnahme unter Behördenvorbehalt. Zusätzlich muss der hessische Datenschutzbeauftragte unterrichtet werden.
Rechtfertigung/Verhältnismäßigkeit: Hier ist die Verhältnismäßigkeit der Maßnahme zu prüfen. Durch die Maßnahme wird in Recht auf informationelle Selbstbestimmung eingegriffen. Eine Überprüfung des Eingriffs anhand des RER-Prüfungsschemas wurde in der Vorlesung durchgeführt und machte deutlich, dass es trotz aller Meinungsverschiedenheiten sinnvoll sein könnte, die präventive Rasterfahndung in Hessen von einem Richtervorbehalt abhängig zu machen.

Anmerkung FÖR: Die Beantwortung hätte in einem flüssigen Text vorgenommen werden sollen. Des weiteren wären z.T. ausführlichere Begriffserklärungen angemessen gewesen.

Teil IV (Multiple-Choice Fragen)- 5 % (je Frage 1 Punkt)

<u>Hinweis</u>: Die richtige(n) Antwort(en) ist (sind) kenntlich zu markieren.

1. Charakteristika des Völkerrechts sind:

a) keine zwangsweise Rechtsdurchsetzung x☐
b) obligatorische Gerichtsbarkeit ☐
c) Konsensprinzip. x☐

2. Das Zivilrecht

a) regelt Vertragsbeziehungen von Privaten x ☐

b) betrifft nur ex-post-Sanktionen ☐

3. Authentische Vertragssprache(n) der CCC ist / sind

a) nur Englisch ☐

b) Französisch und Englisch x ☐

a) Englisch, Französisch und Deutsch ☐

4. Beim strafrechtlichen Prüfungsschema prüft man

a) Objektiver Tatbestand x ☐

b) Formelle Verfassungsmäßigkeit ☐

c) Schuld x ☐

5. Art. 249 EG enthält u.a. Regelungen zu

a) Europäische Richtlinien x ☐

b) OECD-Guidelines ☐

c) Europäische Verordnungen x ☐