Prof. Dr. Viola Schmid, LL.M. (Harvard)

Informations- und Datenschutzrecht I

Modul 2

Datum	Modul	Inhalt
8.11. und 15.11.2005	2	**Rasterfahndung**

A. Sachverhalt 2
B. Geltungsbereich des Datenschutzrechts 4
I. Sachmaterie, Verwaltungsverfahren und Verwaltungsprozess 4
II. Bundes- und Landesverwaltungsverfahrensgesetz 7
III. „Amtshilfe“ nach dem VwVfG neben dem HSOG als besonderem Verwaltungsrecht? 8
IV. Allgemeines und spezielles Datenschutzrecht - (HDSG und HSOG) 11
1. Geltungsbereich des Bundes- oder Landesdatenschutzgesetzes? 11
2. Objektiver Geltungsbereich des HDSG im Verhältnis zum HVwVfG 12
3. Objektiver Geltungsbereich des HDSG im Verhältnis zum HSOG 13
C. Ergebnis 15
D. Aktuelles 16
E. Anhang: §§ 20-26 HSOG 18

A. Sachverhalt

Fallvariante:

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.

Rechtsgrundlage für den automatisierten Datenabgleich ist § 26 HSOG.

§ 26 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. § 29 Abs. 6 Satz 4 und 5 und Abs. 7 gilt entsprechend.

Für die Beurteilung des Sachverhalts sind theoretisch das Hessische Datenschutzgesetz (HDSG), das Hessische Verwaltungsverfahrensgesetz (HVwVfG) und/oder das Hessisches Gesetz über die öffentliche Sicherheit und Ordnung maßgeblich (HSOG).

Die Frage der Verantwortung für die Rechtmäßigkeit des Datenorganisationsverlangens ist im HSOG nicht ausdrücklich geregelt (siehe Anhang F, der die einzelnen Bestimmungen des HSOG enthält). Deshalb ist fraglich,

- ob das HSOG abschließend ist, mit der Folge, dass ein Rückgriff auf Verwaltungsverfahrensgesetz (VwVfG) und allgemeines Datenschutzrecht (DSG) nicht in Betracht kommt. Allein verantwortlich wäre dann die ersuchende Behörde, die Polizei.
- oder ein Rückgriff erfolgt. In Betracht kommen dann vor allem zwei Regelungen:

§ 7 HVwVfG [Durchführung der Amtshilfe]

(2) Die ersuchende Behörde trägt gegenüber der ersuchten Behörde die Verantwortung für die Rechtmäßigkeit der zu treffenden Maßnahme. Die ersuchte Behörde ist für die Durchführung der Amtshilfe verantwortlich

Wenn § 7 S. 1 des Hessischen Verwaltungsverfahrensgesetz gilt, dann ist die Behörde verantwortlich, die das Datenorganisationsverlangen initiiert (§ 7 HVwVfG ist wortlautidentisch mit § 7 VwVfG) – also die Polizei.

§ 14 HDSG [Verantwortlichkeit für die Zulässigkeit der Datenübermittlung]

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

Ist die Übermittlung zur Erfüllung von Aufgaben eines in § 3 Abs. 1 genannten Empfängers erforderlich, so trägt auch dieser hierfür die Verantwortung und hat sicherzustellen, dass die Erforderlichkeit nachträglich überprüft werden kann.

Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen.

Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen.

Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

Wenn § 14 Hessisches Datenschutzgesetz gilt, dann ist die Universität für die Durchführung der Datenorganisation verantwortlich.

Die Frage der Verantwortlichkeit ist also zugleich eine Frage des Verhältnisses dieser Gesetze und des HSOG zueinander

B. Geltungsbereich des Datenschutzrechts

I. Sachmaterie, Verwaltungsverfahren und Verwaltungsprozess

Eine Sachmaterie „Datenschutzrecht“ kennt das Grundgesetz im Kompetenztitel nicht. Das Datenschutzrecht ist eine Querschnittsmaterie und deswegen zunächst und historisch Bestandteil des Verwaltungs(verfahrens)rechts. Durch den Erlass eines Bundesdatenschutzgesetzes und eines (hessischen) Landesdatenschutzgesetzes haben die Gesetzgeber auf Bundes- und Landesebene die datenschutzrechtlichen Anforderungen (die Verwaltungstätigkeit von Behörden betreffend) konkretisiert. Datenschutz- und Datensicherheitsrecht (im Bereich der "Rasterfahndung") ist deshalb **im Schwerpunkt**[1] Verwaltungsverfahrensrecht.

ANFANG§§§§§§§§§§§§§§§§§§§§§ **FEX (Für Experten)** §§§§§§§§§§§§§§§§§§§§§§§§§§

Die Beachtung von Datenschutz und Datensicherheit ist regelmäßig ein Aspekt guter Verwaltung.

Artikel II-101 Europäischer Verfassungsvertrag (VEV)[2] [Recht auf eine gute Verwaltung]

(1) Jede Person hat ein Recht darauf, dass ihre Angelegenheiten von den Organen, Einrichtungen und sonstigen Stellen der Union unparteiisch, gerecht und innerhalb einer angemessenen Frist behandelt werden.

(2) Dieses Recht umfasst insbesondere

a) das Recht jeder Person, gehört zu werden, bevor ihr gegenüber eine für sie nachteilige individuelle Maßnahme getroffen wird,

b) das Recht jeder Person auf Zugang zu den sie betreffenden Akten unter Wahrung des berechtigten Interesses der Vertraulichkeit sowie des Berufs und Geschäftsgeheimnisses,

c) die Verpflichtung der Verwaltung, ihre Entscheidungen zu begründen.

(3) Jede Person hat Anspruch darauf, dass die Union den durch ihre Organe oder Bediensteten in Ausübung ihrer Amtstätigkeit verursachten Schaden nach den allgemeinen Rechtsgrundsätzen ersetzt, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.

Kompetenzrechtlich ist der Datenschutz damit eine Materie des Verwaltungsverfahrensrechts (wenn Behörden handeln). Vom Verwaltungsverfahrensrecht können in einer grundsätzlichen Betrachtung zwei weitere Arten von Gesetzgebung unterschieden werden:

---

[1] Normen wie etwa § 86 a VwGO – die Einführung elektronischer Dokumente in den Verwaltungsprozess - setzten Datenschutz und Datensicherheit voraus.

[2] Vgl. Europäischen Verfassung vom 13.10.2004, die am 29.10.2004 von den Staats- und Regierungschefs der 25 EU-Mitgliedstaaten unterzeichnet wurde. Die Verfassung bedarf zum Inkrafttreten der Ratifizierung durch die Mitgliedstaaten. Dazu Modul 3. Volltext unter: http://europa.eu.int/constitution/index_de.htm

Sachrecht ("materielles Recht")	Verwaltungsverfahrensrecht	Verwaltungsprozessrecht
➢ Etwa: Art. 73 Nr. 7 GG: „Post- und Telekommunikation“	➢ Art. 84 Abs. 1 GG , wenn die Länder Bundesgesetze als eigene Angelegenheit vollziehen ➢ Art. 83 i.V.m. Art. 70 GG, wenn die Länder Landesgesetze vollziehen	➢ Art. 74 Abs. 1 Nr. 1 GG „gerichtliche Verfahren“

Bei der Sachgesetzgebung geht es um die Regelung einer Sachmaterie, beim Verwaltungsverfahren geht es um die Regelung des Vollzugs des Sachgesetzes und bei der Verwaltungsprozessordnung geht es um das Verfahren, wie die Sachgesetzgebung und die Verwaltung gerichtlich kontrolliert werden können. Jenseits der oben vorgestellten Schwerpunktbetrachtung (Verwaltungsverfahrensrecht) können Datenschutz- und Datensicherheitsrecht Teilaspekte aller drei Materien sein.

- Post- und Telekommunikation verlangen Datenschutz und Datensicherheit (Data Privacy and Data Security =DPDS), wie sich nicht erst aus Art. 10 GG ergibt.

- Verwaltung, die mit elektronischen Dokumenten arbeitet, verlangt DPDS:

§ 3a VwVfG [elektronische Kommunikation]

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

(3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

- Prozesse die auf der Grundlage elektronischer Daten geführt werden, verlangen DPDS:

§ 55a VwGO [Elektronische Dokumentenübermittlung]

(1) Die Beteiligten können dem Gericht elektronische Dokumente übermitteln, soweit dies für den jeweiligen Zuständigkeitsbereich durch Rechtsverordnung der Bundesregierung oder der

Landesregierungen zugelassen worden ist. Die Rechtsverordnung bestimmt den Zeitpunkt, von dem an Dokumente an ein Gericht elektronisch übermittelt werden können, sowie die Art und Weise, in der elektronische Dokumente einzureichen sind. Für Dokumente, die einem schriftlich zu unterzeichnenden Schriftstück gleichstehen, ist eine qualifizierte elektronische Signatur nach § 2 Nr. 3 des Signaturgesetzes vorzuschreiben. Neben der qualifizierten elektronischen Signatur kann auch ein anderes sicheres Verfahren zugelassen werden, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Die Landesregierungen können die Ermächtigung auf die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Übermittlung kann auf einzelne Gerichte oder Verfahren beschränkt werden. Die Rechtsverordnung der Bundesregierung bedarf nicht der Zustimmung des Bundesrates.

(2) Ein elektronisches Dokument ist dem Gericht zugegangen, wenn es in der von der Rechtsverordnung nach Absatz 1 Satz 1 und2 bestimmten Art und Weise übermittelt worden ist und wenn die für den Empfang bestimmte Einrichtung es aufgezeichnet hat. Die Vorschriften dieses Gesetzes über die Beifügung von Abschriften für die übrigen Beteiligten finden keine Anwendung. Genügt das Dokument nicht den Anforderungen, ist dies dem Absender unter Angabe der für das Gericht geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen.

(3) Soweit eine handschriftliche Unterzeichnung durch den Richter oder den Urkundsbeamten der Geschäftsstelle vorgeschrieben ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn die verantwortenden Personen am Ende des Dokuments ihren Namen hinzufügen und das Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 des Signaturgesetzes versehen.

§ 55b VwGO [Elektronische Aktenführung]

(1) Die Prozessakten können elektronisch geführt werden. Die Bundesregierung und die Landesregierungen bestimmen jeweils für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an die Prozessakten elektronisch geführt werden. In der Rechtsverordnung sind die organisatorisch-technischen Rahmenbedingungen für die Bildung, Führung und Verwahrung der elektronischen Akten festzulegen. Die Landesregierungen können die Ermächtigung auf die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Akte kann auf einzelne Gerichte oder Verfahren beschränkt werden. Die Rechtsverordnung der Bundesregierung bedarf nicht der Zustimmung des Bundesrates.

(2) Dokumente, die nicht der Form entsprechen, in der die Akte geführt wird, sind in die entsprechende Form zu übertragen und in dieser Form zur Akte zu nehmen, soweit die Rechtsverordnung nach Absatz 1 nichts anderes bestimmt.

(3) Die Originaldokumente sind mindestens bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren.

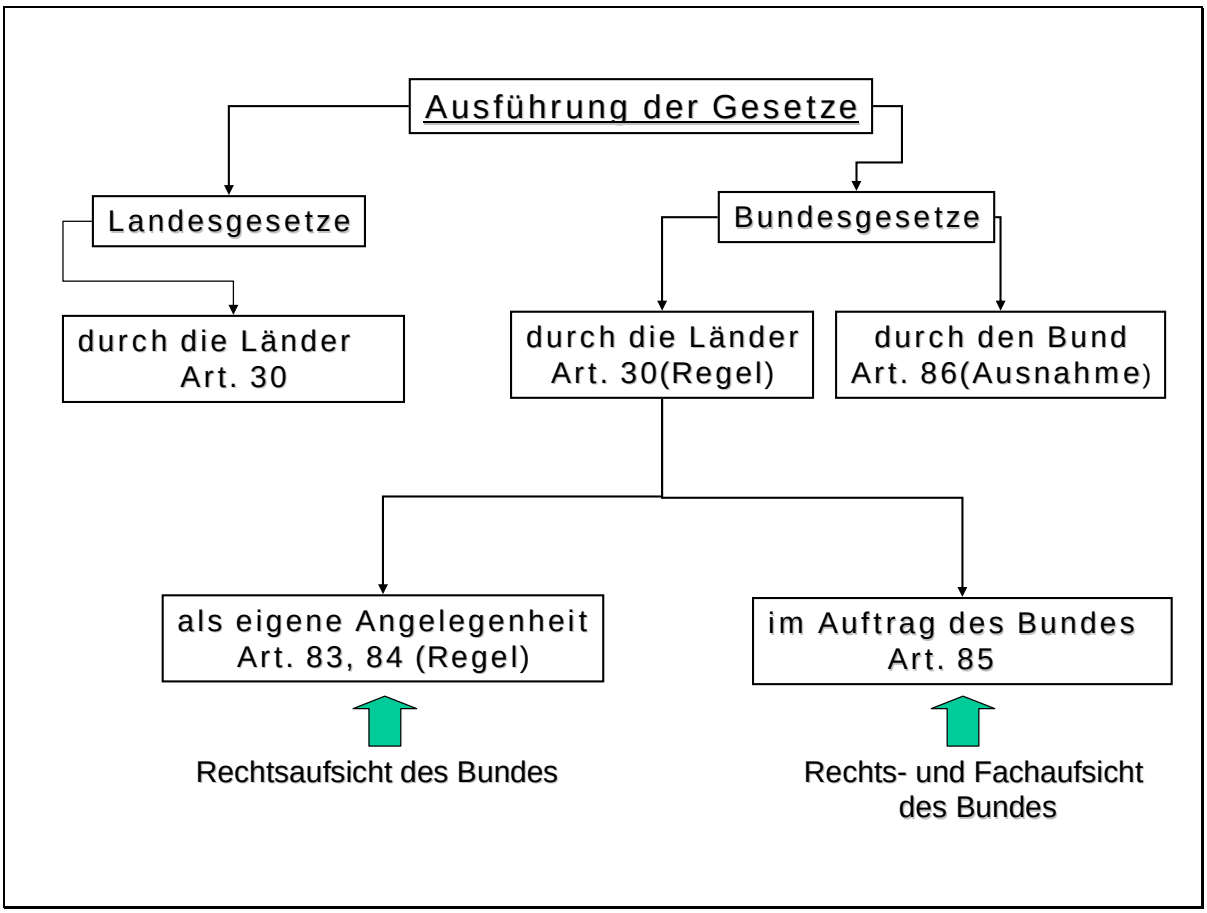
(4) Ist ein in Papierform eingereichtes Dokument in ein elektronisches Dokument übertragen worden, muss dieses den Vermerk enthalten, wann und durch wen die Übertragung vorgenommen worden ist. Ist ein elektronisches Dokument in die Papierform überführt worden, muss der Ausdruck den Vermerk enthalten, welches Ergebnis die Integritätsprüfung des Dokuments ausweist, wen die Signaturprüfung als Inhaber der Signatur ausweist und welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist.

(5) Dokumente, die nach Absatz 2 hergestellt sind, sind für das Verfahren zugrunde zu legen, soweit kein Anlass besteht, an der Übereinstimmung mit dem eingereichten Dokument zu zweifeln.

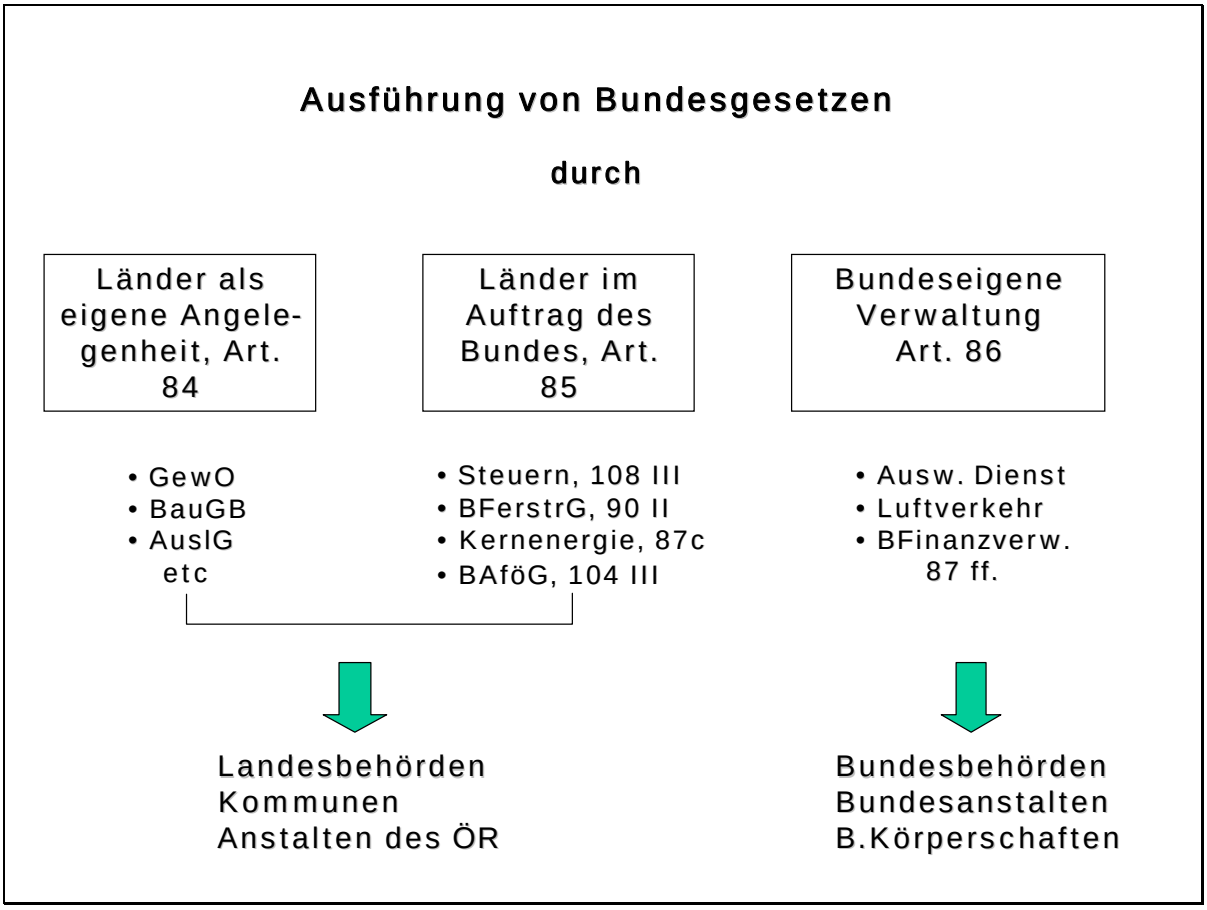
Aus dieser Querschnittseigenschaft ergibt sich das Nebeneinander von – bei einigen Sachverhaltskonstellationen – drei Rechtsgebieten, die Regelung hinsichtlich DPDS enthalten. Das **grundsätzliche horizontale Nebeneinander** von Sachmaterie und Verwaltungsverfahrensgesetz wird noch durch **eine vertikale Ebene** ergänzt – nämlich die unterschiedlichen Bundes- und Landeszuständigkeit im Verwaltungsverfahrensrecht.

II. Bundes- und Landesverwaltungsverfahrensgesetz

FEX[3]



[3] Für Experten.



Je nachdem, ob es sich um eine Materie des Bundes- oder Landesverwaltungsverfahrensgesetzes handelt, ist auch der Geltungsbereich des **Bundes- oder Landesdatenschutzrechts als besonderer Teil des Verwaltungsverfahrensrechts** (Bundes- oder Landesverwaltungsverfahrensrecht) eröffnet (ORIENTIERUNG[4]).

ENDE §§§§§§§§§§§§§§§§§§§§§§§ **FEX (Für Experten)** §§§§§§§§§§§§§§§§§§§§§§§§§§

III. „Amtshilfe“ nach dem VwVfG neben dem HSOG als besonderem Verwaltungsrecht?

Das Besondere an dem Auskunftsverlangen zur Förderung der Rasterfahndung ist, dass **ein** "Verwaltungsverfahren" bei der Polizei (besonderes Verwaltungsrecht) mit den Daten, die in **einem anderen Verwaltungsverfahren** bei der Universität (Immatrikulation …Betreuung der Studenten) „organisiert“ werden, unterstützt werden soll. Grundsätzlich wird die Zusammenarbeit von Behörden nach den Vorschriften des allgemeinen Verwaltungsverfahrensge-

[4] ORIENTIERUNG: So wird eine zusammenfassende Betrachtung charakterisiert, die grundsätzlich und ergebnisorientiert ist. Auf die Notwendigkeit einer detaillierteren Prüfung im Einzelfall wird hingewiesen.

setzes (VwVfG) über die Amtshilfe geregelt: Grundsätzlich ist jede Behörde verpflichtet einer anderen zu helfen (§ 4 Abs. 1 VwVfG).

§ 4 VwVfG [Amtshilfepflicht]
(1) Jede Behörde leistet anderen Behörden auf Ersuchen ergänzende Hilfe (Amtshilfe).

Und grundsätzlich besteht ein großes Interesse der gesamten öffentlichen Hand und Verwaltung, über alle Daten zu verfügen, die in beliebig vielen Verwaltungsverfahren organisiert wurden (etwa Abgleich der Steuerdaten mit den Sozialhilfedaten mit den Daten über Kfz-Zulassungen und mit den Daten der Meldebehörden). In den USA hat das in den siebziger Jahren dazu geführt, dass die Einführung einer möglichst umfassenden Datenbank für die amerikanischen Behörden diskutiert wurde. Die (automatisierte) Organisation von Daten (der "gläserne Mensch") als conditio sine qua non für eine gute Verwaltung? Diesem so augenscheinlich überzeugenden und von der grammatischen Auslegung des § 4 Abs. 1 VwVfG unterstützten Argument stellt das BVerfG (und die Datenschützer) das Recht auf informationelle Selbstbestimmung entgegen. Der berühmte W-Satz (zu wissen, wer, wann, wofür, wo, wie lange, welche Daten organisiert) steht im Gegensatz zu diesem allumfassenden Informationsinteresse des Staates und seiner Untergliederungen. Das Verfassungsrecht (Recht auf informationelle Selbstbestimmung) gebietet deswegen eine restriktive Auslegung von § 4 Abs. 1 VwVfG. Entgegen seinem Wortlaut (contra legem) gilt für Amtshilfe, die in der "Organisation" von Daten besteht, der **„Grundsatz der Amtshilfefestigkeit“**. Mit der Bezeichnung als Grundsatz ist auch die Existenz von Ausnahmen indiziert: Eine Ausnahme ist die spezielle Regelung über die verwaltungsinterne Übermittlung von Daten - etwa durch § 26 HSOG - und/oder eine Einwilligung des Betroffenen (hier des X)[5]. Problematisch wird im Folgenden sein, **inwieweit** die Spezialität einer solchen Regelung gegenüber dem Verwaltungsverfahrensgesetz zu bejahen ist.

Nach hier vertretener Ansicht bedarf es einer - anders als in der Rechtsprechung (jedenfalls im einstweiligen Rechtschutz) geübt[6] - **äußersten Zurückhaltung bei der parallelen Anwendung von Normkomplexen. Grundsätzlich sollen nach hier vertretener Ansicht Gesetze nach dem Effektivitäts- und Effizienzprinzip ausgelegt werden – und diese Auslegungsmaxime steht einer (undifferenzierten) Parallelprüfung von Normen entgegen (Normenflut und Rechtsversagen?).**

[5] Etwa § 31 und des Hessischen Meldegesetzes regelt die Datenübermittlung an andere Behörden.

[6] LG Gießen, Beschluss vom 08.11.2002 Az.:10 G 4501/02 und VGH Kassel, Beschluss vom 04.02.2003 Az.: 10 T 3112/02.

Grundsätzlich ist - anders als von der Rechtsprechung propagiert - immer von der Spezialität auszugehen - und nicht das Nebeneinander von Normkomplexen zum Prinzip zu erklären. Für diese Betrachtung spricht, dass die systematische Auslegung dann an Bedeutung verliert, wenn unterschiedliche Normenkomplexe nebeneinander angewendet werden. Eine Parallelauslegung birgt zudem die Gefahr, dass der Teleologie des Spezialgesetzes nicht ausreichend Rechnung getragen wird.

- Ein unterstützendes Argument für die extensive Spezialität des HSOG als besonderes Verwaltungsrecht gegenüber dem allgemeinen Verwaltungsrecht ist auch § 22 Abs. 5 HSOG. Anders als der Grundsatz der Amtshilfefestigkeit im allgemeinen Verwaltungsverfahrensrecht geht es beim Sicherheits- und Polizeirecht grundsätzlich um die Verhütung von Gefahren durch Datenorganisation. Der Grundsatz der Amtshilfefestigkeit ist hier gerade nicht feststellbar.

§ 22 Abs. 5 HSOG [Datenübermittlung innerhalb des öffentlichen Bereichs]

(5) Andere Behörden und sonstige öffentliche Stellen können personenbezogene Daten an die Gefahrenabwehr- und die Polizeibehörden übermitteln, soweit dies zur Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben erforderlich erscheint und die von der übermittelnden Stelle zu beachtenden Rechtsvorschriften nicht entgegenstehen. Sie sind zur Übermittlung verpflichtet, wenn es für die Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person erforderlich ist.

- .Ein weiteres unterstützendes Argument gegen den Rückgriff auf das VwVfG wäre eine hypothetisch parallele Anwendung von § 26 HSOG und § 5 VwVfG, die im Ergebnis dazu führen würde, dass der Gesetzgeber die Möglichkeit der Rasterfahndung schafft (§ 26 HSOG) und der Behördenleiter B sich darauf berufen könnte, dass die Amtshilfe dem Wohl eines Landes erhebliche Nachteile (§ 5 Abs. 2 Nr. 2 VwVfG) bereiten würde.

§ 5 Abs. 3 VwVfG [Voraussetzungen und Grenzen der Amtshilfe]

(3) Die ersuchte Behörde braucht Hilfe nicht zu leisten, wenn

1. eine andere Behörde die Hilfe wesentlich einfacher oder mit wesentlich geringerem Aufwand leisten kann;
2. sie die Hilfe nur mit unverhältnismäßig großem Aufwand leisten könnte;
3. sie unter Berücksichtigung der Aufgaben der ersuchenden Behörde durch die Hilfeleistung die Erfüllung ihrer eigenen Aufgaben ernstlich gefährden würde

Dies wäre sinnwidrig (teleologische und systematische Auslegung). Grundsätzlich ist deswegen von einer abschließenden Regelung des HSOG im Verhältnis zum VwVfG auszugehen.
Selbst wenn man einer anderen Auffassung folgt, und im **Ausnahmefall bereichsspezifisch** auf das allgemeine Verwaltungsverfahrensrecht zurückgreift, führte das zu keinem anderen

Ergebnis, weil sowohl § 7 S. 1 VwVfG als auch das HSOG (mangels anderweitiger Bestimmung) von der Verantwortlichkeit der ersuchenden Stelle ausgehen.

IV. Allgemeines und spezielles Datenschutzrecht - (HDSG und HSOG)

Die Amtshilfe via Datenorganisation stellt einen besonderen Fall der Amtshilfe dar. Grundsätzlich hat die ersuchte Behörde zu prüfen,

- ob sie dem Amtshilfeersuchen nachkommt und bejahendenfalls
- ein Ermessen, wie sie dem Amtshilfeersuchen nachkommt (Informationstechnik).

Bei § 26 HSOG ist das „Wie“ verengt auf die Organisation und Übermittlung der Daten (wie sich auch aus § 26 Abs. 2 S. 2 HSOG) ergibt. Es handelt sich deshalb um ein tendenziell einstufiges Amtshilfeverfahren, das - wenn die Rasterfahndung effektiv und effizient mit Daten unterstützt werden soll – möglichst weitgehend nach dem HSOG zu interpretieren ist. Eine Anwendbarkeit des (Landes)Datenschutzgesetzes ist wegen der umfangreichen Datenschutzbestimmungen des HSOG (vgl. §§ 20-29 HSOG, Abdruck im Anhang) wiederum allenfalls im Ausnahmefall zu bejahen (**Effektivitäts- und Effizienzprinzip)**. Die grundsätzliche Vermeidung der Parallelanwendung von Normenkomplexen ist auch im Verhältnis HSOG – (H)DSG Postulat. Vor der weiteren Prüfung der Spezialität von HSOG zu Datenschutzrecht ist zunächst zu klären, ob der Geltungsbereich des Bundes- oder des Landesdatenschutzgesetzes eröffnet ist.

1. Geltungsbereich des Bundes- oder Landesdatenschutzgesetzes?

§ 1 BDSG [Zweck und Anwendungsbereich des Gesetzes]

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

a) Bundesrecht ausführen oder

b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Die Universität (etwa die TUD) ist eine öffentliche Stelle des Landes, § 1 Abs. 1 Hessisches Hochschulgesetz.

§ 1 Abs. 1 Hessisches Hochschulgesetz [Rechtsstellung der Hochschulen]

Die Hochschulen des Landes Hessen sind rechtsfähige Körperschaften des öffentlichen Rechts und zugleich staatliche Einrichtungen.(…)

(2) Sie haben das Recht der Selbstverwaltung im Rahmen der Gesetze.(…)

Der Geltungsbereich des Bundesdatenschutzgesetzes ist nicht eröffnet, weil die Universität als staatliche Einrichtung des Landes Hessen kein Bundesrecht ausführt (es handelt sich sowohl beim Verwaltungsverfahrensrecht als auch beim Sicherheit- und Ordnungsrecht um Landesrecht).

§ 3 Abs. 1 HDSG [Anwendungsbereich]

(1) Dieses Gesetz gilt für Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen ungeachtet ihrer Rechtsform. Dieses Gesetz gilt auch für nicht-öffentliche Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der in Satz 1 genannten Stellen wahrnehmen. (…)

Die Universität ist eine "der Aufsicht des Landes unterstehende juristische Person des öffentlichen Rechts“ (§ 1 Abs. 1 in Verbindung mit § 93 Hessisches Hochschulgesetz).

§ 93 Hessisches Hochschulgesetz [Aufsicht]

(1) Das Ministerium kann rechtswidrige Beschlüsse und Maßnahmen beanstanden; es kann dabei eine Frist zur Abhilfe setzen. Beanstandete Beschlüsse und Maßnahmen dürfen nicht ausgeführt werden; sind sie bereits ausgeführt, kann das Ministerium anordnen, dass sie rückgängig gemacht werden.

(2) Erfüllen die zuständigen Stellen die ihnen obliegenden Pflichten nicht, kann das Ministerium anordnen, dass sie innerhalb einer bestimmten Frist das Erforderliche veranlassen.

(3) Die Aufsicht in Auftragsangelegenheiten wird durch Weisung ausgeübt. Vor einer Weisung soll der Hochschule Gelegenheit zur Stellungnahme gegeben werden.

(4) Kommt die Hochschule einer Aufsichtsmaßnahme nicht nach, kann das Ministerium

1. im Fall des Abs. 1 die beanstandeten Beschlüsse und Maßnahmen aufheben,

2. in den Fällen der Abs. 2 und 3 anstelle der Hochschule das Erforderliche veranlassen.

Der Geltungsbereich des HDSG ist für die Universität (§ 3 Abs. 1 S. 1 HDSG) eröffnet.

2. Objektiver Geltungsbereich des HDSG im Verhältnis zum HVwVfG

Bei der Übermittlung der Daten handelt es sich um eine Verarbeitung im Sinne des HDSG (§ 2 Abs. 2 Nr. 3 HDSG).

§ 3 HDSG [Anwendungsbereich]

(2) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

§ 24 HVwVfG [Untersuchungsgrundsatz]

(1) Die Behörde ermittelt den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen; an das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden.

§ 1 HVwVfG [Anwendungsbereich]

(1) Dieses Gesetz gilt für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden

1. des Landes,

2. der Gemeinden und Gemeindeverbände,

3. der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts,

soweit **nicht Rechtsvorschriften des Landes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten**.

Nach § 3 Abs. 2 HDSG und § 1 Abs. 1 HVwVfG (entgegenstehende Bestimmungen in § 7 VwVfG und § 14 HDSG) gehen die Bestimmungen des HDSG denen des HVwVfG vor, wenn es sich bei der Ermittlung des Sachverhalts um die Verarbeitung personenbezogener Daten handelt. Die Vorlesung geht deswegen grundsätzlich von einer Spezialität des Datenschutzgesetzes vor dem Verwaltungsverfahrensgesetz aus.

3. Objektiver Geltungsbereich des HDSG im Verhältnis zum HSOG

Der objektive Geltungsbereich des HDSG könnte aufgrund der spezielleren Rechtsvorschriften im HSOG nicht eröffnet sein.

§ 3 Abs. 3 HDSG

(3) Soweit besondere Rechtsvorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten vorhanden sind, gehen sie den Vorschriften dieses Gesetzes vor.

Die Vielzahl der oben zitierten und im Anhang abgedruckten Bestimmungen des HSOG (§§ 20-29 HSOG) über die Datenorganisation führt nach hier vertretener Ansicht dazu, dass grundsätzlich eine Spezialität des HSOG vor dem HDSG anzunehmen ist. Nur insoweit als das HSOG keine Bestimmung enthält, ist auf das HDSG zu rekurrieren. Für die Verantwortlichkeit enthält das HSOG keine ausdrückliche Bestimmung. Eine abschließende Regelung (wie im Verhältnis zum HVwVfG) ist im Verhältnis zum HDSG nach hier vertretener Ansicht

nicht zu bejahen, weil die Frage der Verwantwortlichkeit insbesondere hinsichtlich des Prüfungsumfangs im HDSG speziell geregelt ist.

§ 14 HDSG [Verantwortlichkeit für die Zulässigkeit der Datenübermittlung]

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Ist die Übermittlung zur Erfüllung von Aufgaben eines in § 3 Abs. 1 genannten Empfängers erforderlich, so trägt auch dieser hierfür die Verantwortung und hat sicherzustellen, dass die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen.Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

§ 14 HDSG regelt zwei Szenarien.

- § 14 S. 1 HSDG „einfache“ Übermittlung
- § 14 S. 2-5 HDSG „Übermittlung zur Erfüllung von Aufgaben öffentlicher Stellen“

§ 3 HDSG [Anwendungsbereich]

(1) Dieses Gesetz gilt für Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen ungeachtet ihrer Rechtsform. Dieses Gesetz gilt auch für nicht-öffentliche Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der in Satz 1 genannten Stellen wahrnehmen.

(2) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(3) Soweit besondere Rechtsvorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten vorhanden sind, gehen sie den Vorschriften dieses Gesetzes vor.

(4) Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind sowie für Daten des Betroffenen, die von ihm zur Veröffentlichung bestimmt sind.

(5) Soweit der Hessische Rundfunk personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet, gelten von den Vorschriften dieses Gesetzes nur die §§ 10 und 37. 2Im übrigen gelten die Vorschriften dieses Gesetzes.

(6) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der Zweite Teil sowie die §§ 34 und 36 dieses Gesetzes. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde sind im übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anwendbar.

Für die Rasterfahndung ist die Datenübermittlung zur Erfüllung der präventiven Aufgabe der Polizei „zur Verhütung von Straftaten“ erforderlich. Es kommt deswegen zu einer „Verantwortungsteilung“. § 14 S. 2 HDSG bestimmt in diesem Fall, dass die Verantwortung für die Übermittlung bei beiden Stellen liegt. Den Umfang der Prüfung bestimmt § 14 S. 3 HDSG.

Zu prüfen sind die

- Zuständigkeit
- Schlüssigkeit.

Die ersuchende Stelle hat der übermittelnden Stelle die Informationen darzulegen, die diese braucht, um die Zuständigkeit und die Schlüssigkeit bestimmen zu können (§ 14 S. 5 HDSG).

- Die Schlüssigkeit bedeutet, dass der von der ersuchenden Stelle vorgebrachte Sachverhalt die Datenübermittlung rechtfertigt. Das heißt, die Polizei muss darlegen, dass der Tatbestand des § 26 HSOG erfüllt ist. Eine weitergehende Prüfung obliegt der übermittelnden Stelle nicht (Umkehrschluss aus § 14 S. 3 HDSG). Dafür spricht auch, dass für eine weitergehende Prüfung die übermittelnde Stelle weitergehende Informationen bräuchte. § 14 S. 4 HDSG bestimmt im Falle des Zweifels an der Schlüssigkeit, dass die Universität noch die Erforderlichkeit prüfen kann. Erforderlichkeit ist in einer systematischen Auslegung als die Erforderlichkeit im Sinn des § 11 HDSG auszulegen.

§ 11 HDSG [Erforderlichkeit]

(1) Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Die Erforderlichkeit einer Datenübermittlung muss bei einer der beteiligten Stellen vorliegen.

C. Ergebnis

Die Vorlesung gelangt zu dem Ergebnis, dass § 14 HDSG anzuwenden ist (weil das HSOG keine Regelung enthält).

§ 14 HDSG ist allerdings nach hier vertretener Ansicht verfassungskonform hinsichtlich der Prüfungsbefugnis extensiver auszulegen. Die Schlüssigkeit ist im Lichte des Rechts auf informationelle Selbstbestimmung zu konkretisieren. Grundsätzlich gibt es nach § 26 HSOG in Verbindung mit § 14 HDSG zwei Möglichkeiten:

- Die Universität geht von der Zuständigkeit der ersuchenden Behörde und der "Schlüssigkeit" des Ersuchens aus (§ 14 S. 3 HDSG), die auch von der Begründung des Organisationsverlangens der Polizei abhängt - eine weitere Prüfung und Verantwortlichkeit der Universität ergibt sich nicht.
- Es drängen sich Zweifel an der Zuständigkeit oder der Schlüssigkeit auf - dann ist die Universität berechtigt, die Erforderlichkeit - und damit weitergehend als die Fehlerevidenzkontrolle des § 14 S. 3 HDSG - zu prüfen (§ 14 S. 4 HDSG). Aus verfassungsrechtlicher Sicht liegt es nahe, nicht nur ein solches Prüfungsrecht - sondern sogar eine Prüfungs-

pflicht - zu fordern - insbesondere seit dem Wegfall des Richtervorbehalts in § 26 Abs. 4 HSOG.

In der Klausur wären beide Lösungen vertretbar.

D. Aktuelles

Das Thema Rasterfahndung ist nach wie vor hochaktuell: In Hessen wurde am 15.12.2004 das HSOG geändert und folgender § 14 Abs. 5 HSOG eingefügt:

§ 14 HSOG [Datenerhebung und sonstige Datenverarbeitung an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen]

(V) Die Polizeibehörden können auf öffentlichen Straßen und Plätzen Daten von Kraftfahrzeugkennzeichen zum Zwecke des Abgleichs mit dem Fahndungsbestand automatisiert erheben. Daten, die im Fahndungsbestand nicht enthalten sind, sind unverzüglich zu löschen.

Die automatisierte Kennzeichenerkennung stellt zwar keine Rasterfahndung im engeren Sinne dar, wie sie soeben dargestellt wurde, hat aber mit der Rasterfahndung das Charakteristikum des Datenabgleichs gemein. Daneben trägt die automatisierte Kennzeichenerkennung auch Züge der Schleierfahndung (verdachtsunabhängige Personenkontrolle), nämlich die Verdachts- und Anlasslosigkeit der Maßnahme. In der Sache geht es um die gleichen Fragestellungen und Herausforderungen wie bei der Rasterfahndung im engeren Sinne:

- Verdecktheit der Maßnahme:

  Die Kennzeichenerkennung erfolgt verdeckt. Keiner der Betroffenen kann erkennen, wann und wo er von einer solchen Maßnahme erfasst wird. Eine nachträgliche Überprüfung der Rechtmäßigkeit der Maßnahme wird dem Bürger damit unmöglich.

- (Fehlende) Bestimmtheit der Norm:

  Der Zweck der Datenerhebung „zum Abgleich mit dem Fahndungsbestand“ ist zwar genannt, konkrete Datenbestände sind aber nicht genannt. Eine Einschränkung oder nähere Bestimmung der Orte, an denen eine Kennzeichenerfassung ermöglicht wird, existiert nicht; jeder öffentliche Platz und jede öffentliche Straße kann Ort der polizeilichen Maßnahme sein. Einen konkreten Anlass für die Durchführung einer Kennzeichenerfassung fordert der Gesetzeswortlaut nicht.

- Grundrecht auf informationelle Selbstbestimmung:

  Kfz-Kennzeichen stellen personenbezogene Daten dar. Ihr Zweck liegt gerade darin, dass einem bestimmten Fahrzeug unzweifelhaft ein Halter zugeordnet werden kann. Die Schwere des Eingriffs ergibt sich zum einen aus der Vielzahl der Betroffenen. Zum anderen wird

die möglicherweise nur geringe Qualität des Eingriffs durch die Quantität der Eingriffe – wegen der oftmals wiederholten Betroffenheit – aufgewogen.

- Eröffnung des Geltungsbereichs weiterer Grundrechte:
  Die Grundechte auf körperliche Bewegungsfreiheit (Art. 2 Abs. 2 S. 2 GG) und auf Freizügigkeit (Art. 11 GG) können dadurch beeinträchtigt werden, dass der Bürger „freiwillig" von seinem Recht auf Bewegungsfreiheit keinen Gebrauch macht, um nicht beobachtet und registriert zu werden.
- Zuständigkeit:
  Der Landesgesetzgeber hat nur für die präventive Gefahrenabwehr eine Gesetzgebungskompetenz. Im Bereich der repressiven Strafverfolgung hat der Bundesgesetzgeber mit der Strafprozessordnung eine abschließende Regelung getroffen. Der Schwerpunkt von Fahndungsmaßnahmen liegt regelmäßig im Bereich der Strafverfolgung.
- Verhältnismäßigkeit im engeren Sinne:
  Die anlass- und verdachtsunabhängige Kennzeichenerfassung betrifft eine Vielzahl von Bürgern, sei es als Kfz-Halter oder sei es als Fahrer. Auf die fehlende Transparenz und der sich daraus ergebenden fehlenden Kontroll- und Überprüfungsmöglichkeit wurde bereits hingewiesen. Die durch die automatisierte Kennzeichenerfassung zu erzielenden Vorteile müssten die sich aus der Maßnahme ergebenden Nachteile überwiegen.

Der Hessische Staatsgerichtshof, bei dem derzeit eine Grundrechtsklage zur Verfassungsmäßigkeit von § 14 Abs. 5 HSOG anhängig ist, wird sich mit diesen Problemen auseinandersetzen.

E. Anhang: §§ 20-26 HSOG

§ 20 HSOG [Datenspeicherung und sonstige Datenverarbeitung]

(1) Die Gefahrenabwehr- und die Polizeibehörden können erhobene personenbezogene Daten speichern und sonst verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Dies gilt auch für personenbezogene Daten, die die Gefahrenabwehr- und die Polizeibehörden unaufgefordert durch Dritte erlangt haben.

(2) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen von den Gefahrenabwehr- und den Polizeibehörden nicht für andere Zwecke verwendet werden, es sei denn, dies ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich oder es liegen tatsächliche Anhaltspunkte dafür vor, dass ohne ihre Verarbeitung die Verhütung oder die Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person aussichtslos oder wesentlich erschwert wäre.

(3) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten über andere als die in § 13 Abs. 2 Nr. 1 genannten Personen nur zu den Zwecken speichern und sonst verarbeiten, zu denen sie die Daten erlangt haben. Die Verarbeitung zu einem anderen gefahrenabwehrbehördlichen oder polizeilichen Zweck ist zulässig, soweit die Gefahrenabwehr- und die Polizeibehörden die Daten auch zu diesem Zweck hätten erheben und noch verarbeiten können.

(4) Die Polizeibehörden können, soweit Bestimmungen der Strafprozessordnung oder andere gesetzliche Regelungen nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten speichern oder sonst verarbeiten. Die Speicherung oder sonstige Verarbeitung in automatisierten Verfahren ist nur zulässig, wenn es sich um Daten von Personen handelt, die verdächtig sind, eine Straftat begangen zu haben; entfällt der Verdacht, sind die Daten zu löschen.

(5) Die Polizeibehörden können zur Verhütung von Straftaten personenbezogene Daten über die in § 13 Abs. 2 Nr. 2 genannten Personen sowie über Zeuginnen und Zeugen, Hinweisgeberinnen und Hinweisgeber und sonstige Auskunftspersonen automatisiert nur speichern und sonst verarbeiten, soweit dies zur Verhütung von Straftaten mit erheblicher Bedeutung unerläßlich ist. Die Speicherungsdauer darf drei Jahre nicht überschreiten. Nach jeweils einem Jahr, gerechnet vom Zeitpunkt der letzten Speicherung, ist zu prüfen, ob die Voraussetzungen nach Satz 1 noch vorliegen; die Entscheidung, daß eine weitere Speicherung erforderlich ist, trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(…)

§ 21 HSOG [Allgemeine Regeln der Datenübermittlung]

(1) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten, soweit nachstehend nichts anderes bestimmt ist, nur zu dem Zweck übermitteln, zu dem sie die Daten erlangt haben. Empfängerinnen oder Empfänger, Tag und wesentlicher Inhalt der Übermittlung sind festzuhalten; dies gilt nicht für das automatisierte Abrufverfahren (§ 24).

(2) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der Gefahrenabwehr- oder der Polizeibehörde von der zur Verschwiegenheit verpflichteten Person oder Stelle in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, so ist die Übermittlung durch diese Behörden nur zulässig, wenn die Empfängerin oder der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die Gefahrenabwehr- oder die Polizeibehörde erhoben hat oder hätte erheben können. In die Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs muß die zur Verschwiegenheit verpflichtete Person oder Stelle einwilligen.

(3) Bewertungen (§ 20 Abs. 6) dürfen anderen als Gefahrenabwehr- und Polizeibehörden nicht übermittelt werden. Dies gilt nicht, soweit Fahndungsaufrufe mit einer Warnung verbunden sind.

(4) Die Übermittlung darf nicht zu einer Erweiterung des Kreises der Stellen nach § 41 des Bundeszentralregistergesetzes führen, die von Eintragungen, die in ein Führungszeugnis nicht aufgenommen werden, Kenntnis erhalten, und muß das Verwertungsverbot im Bundeszentralregister getilgter oder zu tilgender Eintragungen nach §§ 51 und 52 des Bundeszentralregistergesetzes berücksichtigen.

(5) Die übermittelnde Gefahrenabwehr- oder Polizeibehörde prüft die Zulässigkeit der Übermittlung. Erfolgt die Übermittlung auf Grund eines Ersuchens der Empfängerin oder des Empfängers, hat die übermittelnde Stelle nur zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der Empfängerin oder des Empfängers liegt.

Die Zulässigkeit der Übermittlung im übrigen prüft sie nur, wenn hierfür im Einzelfall besonderer Anlaß besteht. Die Empfängerin oder der Empfänger hat der übermittelnden Stelle die erforderlichen Angaben zu machen.

(6) Die Empfängerin oder der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verarbeiten, zu dem sie ihr oder ihm übermittelt worden sind.

(7) Anderweitige besondere Rechtsvorschriften über die Datenübermittlung bleiben unberührt.

§ 22 HSOG [Datenübermittlung innerhalb des öffentlichen Bereichs]

(1) Zwischen den Polizeibehörden können personenbezogene Daten übermittelt werden, soweit sie diese in Erfüllung ihrer Aufgaben nach § 1 erlangt haben und die Datenübermittlung zur Erfüllung dieser Aufgaben erforderlich ist. Dies gilt auch für die Übermittlung personenbezogener Daten an Polizeibehörden und -dienststellen des Bundes und der anderen Länder. Zwischen den Gefahrenabwehrbehörden, anderen für die Gefahrenabwehr zuständigen Behörden oder öffentlichen Stellen und den Polizeibehörden können personenbezogene Daten übermittelt werden, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich erscheint. § 20 Abs. 3 gilt entsprechend. Liegen die Voraussetzungen nach Satz 1 bis 4 nicht vor, ist Abs. 2 anzuwenden.

(2) Im übrigen können die Gefahrenabwehr- und die Polizeibehörden personenbezogene Daten an Behörden oder öffentliche Stellen übermitteln, soweit dies erforderlich ist

1. zur Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben,

2. zur Abwehr einer Gefahr für die empfangende Stelle,

3. auf Grund tatsächlicher Anhaltspunkte zur Wahrnehmung einer sonstigen Gefahrenabwehraufgabe durch die empfangende Stelle,

4. zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder

5. zur Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person.

In den Fällen des Satz 1 Nr. 5 ist die Person, deren Daten übermittelt worden sind, zu unterrichten, sobald der Zweck der Übermittlung dem nicht mehr entgegensteht.

(3) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, soweit dies zur

1. Erfüllung einer Aufgabe der übermittelnden Gefahrenabwehr- oder Polizeibehörde oder

2. Abwehr einer erheblichen Gefahr durch die empfangene Stelle

erforderlich ist. Die Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines deutschen Gesetzes verstoßen würde oder schutzwürdige Belange der betroffenen Person beeinträchtigt würden. Die empfangende Stelle ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck genutzt werden dürfen, zu dessen Erfüllung sie ihr übermittelt wurden. Die Prüfung der Zulässigkeit der Übermittlung obliegt der übermittelnden Behörde.

(4) Abweichend von § 21 Abs. 1 Satz 1 und Abs. 3 können die Gefahrenabwehr- und die Polizeibehörden personenbezogene Daten nach Maßgabe der Abs. 2 und 3 übermitteln, soweit dies zur Abwehr einer Gefahr unerläßlich ist und die empfangende Stelle die Daten auf andere Weise, obwohl berechtigt, nicht oder nicht rechtzeitig oder nur mit unverhältnismäßig hohem Aufwand erlangen kann.

(…)

§ 23 HSOG [Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs]

(1) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies zur

1. Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben,

2. Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder

3. Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person

erforderlich ist.

(2) § 22 Abs. 2 Satz 2 und Abs. 4 gilt entsprechend.

(3) Die Empfängerin oder der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dessen Erfüllung sie ihr oder ihm übermittelt wurden. Die Prüfung der Zulässigkeit der Übermittlung obliegt der übermittelnden Behörde.

(4) Über die Übermittlungen ist ein besonderes Verzeichnis zu führen, aus dem der Zweck der Übermittlung, die Empfängerin oder der Empfänger und die Aktenfundstelle hervorgehen. Es ist am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu vernichten.

§ 24 HSOG [Automatisiertes Abrufverfahren]

(1) Die Einrichtung eines Verfahrens, das die automatisierte Übermittlung personenbezogener Daten der Polizeibehörden und der Gefahrenabwehrbehörden durch Abruf ermöglicht, ist zulässig, soweit diese Form der Datenübermittlung unter Berücksichtigung der schutzwürdigen Belange der betroffenen Person und der Erfüllung von Aufgaben der beteiligten Stellen angemessen ist. Zum Abruf können zugelassen werden:

1. Polizeibehörden,

2. die Polizeieinrichtung und die Verwaltungsfachhochschule,

3. Polizeibehörden und -dienststellen des Bundes und der anderen Länder,

4. Gefahrenabwehrbehörden in Verfahren, die Zuverlässigkeitsüberprüfungen zum Gegenstand haben

5. Ausländerbehörden in Verfahren, die die Erteilung von Aufenthaltsgenehmigungen und Aufenthaltsbeendigungen zum Gegenstand haben,

6. Einbürgerungsbehörden in Verfahren, die die Ermittlungen von Einbürgerungsvoraussetzungen zum Gegenstand haben

7. die Allgemeinheit, soweit es sich um personenbezogene Daten handelt, die für die Öffentlichkeit bestimmt sind.

In den Fällen des Satzes 2 Nr. 4 bis 6 darf nur Auskunft erteilt werden, wenn über die betroffene Person keine Daten gespeichert sind (Negativauskunft).

(2) Die nach § 10 des Hessischen Datenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen sind schriftlich festzulegen.

(3) Die speichernde Stelle hat in den Fällen von Abs. 1 Satz 2 Nr. 1 bis 6 zu gewährleisten, dass die Übermittlung zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

§ 25 HSOG [Datenabgleich]

(1) Die Polizeibehörden können personenbezogene Daten der in den §§ 6 und 7 sowie § 13 Abs. 2 Nr. 1 genannten Personen mit automatisiert gespeicherten Daten der Polizeibehörden abgleichen. Personenbezogene Daten anderer Personen kann die Polizeibehörde nur abgleichen, wenn dies auf Grund tatsächlicher Anhaltspunkte zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich erscheint. Die Polizeibehörden können ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. Die betroffene Person kann angehalten und für die Dauer des Datenabgleichs festgehalten werden. § 18 bleibt unberührt.

(2) Die Gefahrenabwehrbehörden können personenbezogene Daten mit ihren automatisiert gespeicherten Daten unter den Voraussetzungen für die Verarbeitung personenbezogener Daten (§ 20) abgleichen.

(3) Besondere Rechtsvorschriften über den Datenabgleich bleiben unberührt

§ 26 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. § 29 Abs. 6 Satz 4 und 5 und Abs. 7 gilt entsprechend.

§ 27 HSOG [Berichtigung, Löschung und Sperrung von Daten]

(1) Automatisiert gespeicherte personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, daß in Akten gespeicherte personenbezogene Daten unrichtig sind, ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Automatisiert gespeicherte personenbezogene Daten sind zu löschen und die dazugehörigen Unterlagen sind zu vernichten, wenn

1. ihre Speicherung unzulässig ist oder

2. bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aus Anlaß einer Einzelfallbearbeitung festgestellt wird, daß ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, kann an die Stelle der Löschung die Sperrung treten.

(3) Sind personenbezogene Daten in Akten gespeichert, sind sie im Falle des Abs. 2 Satz 1 Nr. 1 durch Anbringung eines entsprechenden Vermerks zu sperren. Im Fall des Abs. 2 Satz 1 Nr. 2 sind die Akten spätestens zu vernichten, wenn die gesamte Akte zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben nicht mehr erforderlich ist.

(4) Die Ministerin oder der Minister des Innern wird ermächtigt, durch Rechtsverordnung die Fristen zu regeln, nach deren Ablauf zu prüfen ist, ob die weitere Speicherung der Daten zur Aufgabenerfüllung erforderlich ist. Bei Daten, die nach § 20 Abs. 4 automatisiert oder in personenbezogen geführten Akten gespeichert sind, dürfen die Fristen

a) bei Erwachsenen zehn Jahre,

b) bei Jugendlichen fünf Jahre und

c) bei Kindern zwei Jahre

nicht überschreiten, wobei nach Art und Zweck der Speicherung sowie Art und Bedeutung des Anlasses zu unterscheiden ist. Die Frist beginnt regelmäßig mit dem letzten Anlaß der Speicherung, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentzug verbundenen Maßregel der Besserung oder Sicherung.

(5) Stellt die Gefahrenabwehr- oder die Polizeibehörde fest, daß unrichtige oder nach Abs. 2 Satz 1 Nr. 1 zu löschende oder nach Abs. 3 Satz 1 zu sperrende personenbezogene Daten übermittelt worden sind, ist der Empfängerin oder dem Empfänger die Berichtigung, Löschung oder Sperrung mitzuteilen. Die Mitteilung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte bestehen, daß dadurch schutzwürdige Belange der betroffenen Person beeinträchtigt werden können.

(6) Löschung und Vernichtung unterbleiben, wenn

1. Grund zu der Annahme besteht, daß schutzwürdige Belange der betroffenen Person beeinträchtigt würden,

2. die Daten zur Behebung einer bestehenden Beweisnot unerläßlich sind oder

3. die Verarbeitung der Daten, die zum frühestmöglichen Zeitpunkt zu anonymisieren sind, zu wissenschaftlichen Zwecken erforderlich ist.

In diesen Fällen sind die Daten zu sperren und mit einem Sperrvermerk zu versehen.

(7) Gesperrte Daten dürfen nur zu den in Abs. 6 Satz 1 genannten Zwecken oder sonst mit Einwilligung der betroffenen Person verwendet werden.

(8) Anstelle der Löschung und Vernichtung nach Abs. 2 Satz 1 Nr. 2 oder Abs. 3 Satz 2 können die Datenträger an ein öffentliches Archiv abgegeben werden, soweit besondere archivrechtliche Regelungen dies vorsehen.

§ 28 HSOG [Verfahrensverzeichnis]

(1) Wer für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten zuständig ist, hat ein für den behördlichen Datenschutzbeauftragten bestimmtes Verfahrensverzeichnis zu erstellen. Sein Inhalt bestimmt sich nach § 6 Abs. 1 Nr. 1 bis 5 sowie 7 und 8 des Hessischen Datenschutzgesetzes. Es hat außerdem Prüffristen nach § 27 Abs. 2 Satz 1 Nr. 2 zu enthalten.

(2) Die Angaben des Verfahrensverzeichnisses können bei der datenverarbeitenden Stelle von jeder Person eingesehen werden, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird oder die datenverarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt. § 29 Abs. 5 Satz 1 gilt entsprechend.

(3) Sind nach besonderen Rechtsvorschriften Verfahrensverzeichnisse oder Errichtungsanordnungen zu erstellen, treten diese an die Stelle des Verfahrensverzeichnisses nach Abs. 1.

§ 29 HSOG [Auskunft und Unterrichtung]

(1) Der betroffenen Person ist auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,

2. die Herkunft der Daten und die Empfängerinnen oder die Empfänger von Übermittlungen, soweit dies festgehalten ist,

3. den Zweck und die Rechtsgrundlage der Speicherung und sonstigen Verarbeitung.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Bei einem Antrag auf Auskunft aus Akten kann erforderlichenfalls verlangt werden, daß Angaben gemacht werden, die das Auffinden der Daten ohne einen Aufwand ermöglichen, der außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Kommt die betroffene Person dem Verlangen nicht nach, kann der Antrag abgelehnt werden. Statt einer Auskunft über Daten in Akten können die Gefahrenabwehr- und die Polizeibehörden der betroffenen Person Akteneinsicht gewähren.

(2) Abs. 1 gilt nicht für Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden.

(3) Abs. 1 gilt außerdem nicht, soweit eine Abwägung ergibt, daß die dort gewährten Rechte der betroffenen Person hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung insoweit nicht, als durch die Mitteilung der Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

(5) Wird Auskunft nicht gewährt, ist die betroffene Person darauf hinzuweisen, daß sie sich an die Datenschutzbeauftragte oder den Datenschutzbeauftragten wenden kann. Dies gilt nicht in den Fällen des Abs. 1 Satz 4. Die Mitteilung der Datenschutzbeauftragten oder des Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern sie nicht einer weitergehenden Auskunft zustimmt.

(6) Wurden personenbezogene Daten durch eine verdeckte Datenerhebung erlangt, sind die betroffenen Personen hierüber nach Abschluss der Maßnahme auch ohne Antrag zu unterrichten. Betroffen sind die Person, gegen die sich die Maßnahme gerichtet hat, deren Gesprächspartner sowie der Inhaber einer Wohnung in den Fällen des § 15 Abs. 4. Die Unterrichtung unterbleibt, soweit dies im überwiegenden Interesse der Person liegt, gegen die sich die Maßnahme gerichtet hat, oder wenn die Ermittlung der betroffenen Person oder deren Anschrift einen unverhältnismäßigen Verwaltungsaufwand erfordern würde. Eine Unterrichtung unterbleibt ferner, solange sie den Zweck der Maßnahme, ein sich an den auslösenden Sachverhalt anschließendes strafrechtliches Ermittlungsverfahren oder Leib, Leben oder Freiheit einer Person gefährden würde. [5]Die Entscheidungen nach Satz 3 und 4 trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter. Über die Zurückstellung der Unterrichtung ist der Hessische Datenschutzbeauftragte spätestens sechs Monate nach Abschluss der Maßnahme und danach in halbjährlichen Abständen in Kenntnis zu setzen.

(7) Sind die personenbezogenen Daten in ein anhängiges Strafverfahren eingeführt, so ist vor Erteilung der Auskunft die Zustimmung der Staatsanwaltschaft herbeizuführen.