



15. Wahlperiode

Drucksache **15/2949**

HESSISCHER LANDTAG

18. 09. 2001

Stellungnahme der Landesregierung

**betreffend den Neunundzwanzigsten Tätigkeitsbericht
des Hessischen Datenschutzbeauftragten**

Drucksache 15/2500

Inhaltsverzeichnis

Stellungnahme zu:	Seite
4. Videüberwachung	3
4.2 Verkehrsüberwachung durch Videoaufzeichnungen	3
5. Justiz Speicherung personenbezogener Daten auf Richterarbeits- plätzen (elektronisch und in Papierform)	3
6. Polizei- und Strafverfolgungsbehörden	4
6.1 Mangelnde Verwertung des Verfahrensergebnisses bei Datenspeicherungen durch die Polizei	4
6.1.1 Verweigerung begehrter Berichtigung	4
6.1.3 Unterbleibende Löschung trotz Freispruch	4
6.1.4 Unzureichende Sachstandsmitteilung durch die Staats- anwaltschaft	5
6.1.5 Die Rechtslage	5
6.1.6 Fazit	5
6.2 Medienpräsenz bei behördlichen Kontrollen und polizei- lich angeordneten Maßnahmen	6
6.3 Verarbeitung der Hessischen Polizeidaten beim Bundes- kriminalamt im Wege der Datenverarbeitung im Auftrag	6
11. Entwicklungen im Bereich der Technik	7
11.1 Schwachstellensuche bei Firewalls und in Rechnerzentren	7
11.1.2.1 Ergebnisse der Schwachstellenanalyse	7
12. Ausländerrecht	7
12.2 Kontrolle der Ausländerbehörde des Rheingau-Taunus- Kreises	7
12.2.1 Verfahren bei der Ermittlung der so genannten Scheinehen	7
13. Melderecht	8
13.2 Datenübermittlungen der Einwohnermeldeämter an die Gebühreneinzugszentrale	8

Zu 4. Videüberwachung
Zu 4.2 Verkehrsüberwachung durch Videoaufzeichnungen

Die Kritik des Datenschutzbeauftragten beruht auf Missverständnissen.

Durch das Bildmaterial des privaten Fernsehsenders konnte der Eindruck entstehen, als seien die Videoaufnahmen ohne Unterbrechung erfolgt. Nach dem Bericht des betroffenen Polizeipräsidiums wurde und wird der Verkehr jedoch nur dann aufgezeichnet, wenn der Verdacht eines Verkehrsverstößes besteht. Anschließend schaltet der Beamte die Kamera wieder in den "Standby-Modus", sofern nicht sofort der nächste Verkehrsverstoß zu dokumentieren ist.

Der Fall wurde zum Anlass genommen, dem Datenschutzbeauftragten bei der Hessischen Polizeischule die aktuelle Technik zur Verkehrsüberwachung vorzuführen. Dabei wurde ihm dargelegt, dass es derzeit noch keine technischen Geräte gibt, die den fließenden Verkehr analysieren und allein bei Verkehrsverstößen wie Geschwindigkeitsüberschreitungen und Abstandsunterschreitungen auswertbare Bilder aufnehmen.

Als Ergebnis der Besprechung konnte volles Einvernehmen erzielt werden. Der Datenschutzbeauftragte erklärte die Angelegenheit für erledigt. Ihm wurde seitens des Ministeriums des Innern und für Sport zugesagt, jeweils zeitnah über technische Neuentwicklungen informiert zu werden, so dass bei der Geräteeukonzeption durch frühzeitigen Meinungsaustausch Datenschutzgesichtspunkte bestmöglich berücksichtigt werden können.

Zu 5. Justiz
Speicherung personenbezogener Daten auf Richterarbeitsplätzen (elektronisch und in Papierform)

Der Datenschutzbeauftragte vertritt die Auffassung, dass die längerfristige Speicherung von Entscheidungsentwürfen auf den PCs der Richterinnen und Richter, aber auch die Aufbewahrung von Entscheidungskopien in Papierform, zur Verwendung in zukünftigen vergleichbaren Verfahren mangels Rechtsgrundlage nur in anonymisierter Form zulässig ist.

Ihm ist zuzustimmen, dass auch die Organe der Rechtspflege Adressaten der Regelungen des Hessischen Datenschutzgesetzes sind. Dem steht die richterliche Unabhängigkeit nicht entgegen. Gleichwohl muss der Forderung nach Anonymisierung entgegengetreten werden, da sie einerseits einen unverhältnismäßigen Arbeitsaufwand bedeutet, zum anderen aber der Nutzen für den Betroffenen nicht ersichtlich ist.

Der Datenschutzbeauftragte rügt die elektronische Speicherung von personenbezogenen Daten in Urteilsentwürfen ebenso wie die Aufbewahrung von Kopien in Papierform.

In der gerichtlichen Lebenswirklichkeit hält sich jedoch nahezu jede Richterin und jeder Richter zum persönlichen oder kammerinternen/senatsinternen Gebrauch Entscheidungssammlungen – gleich ob in elektronischer oder Papierform. Sofern darin Kopien oder Entwürfe eigener Entscheidungen enthalten sind, sind diese regelmäßig nicht anonymisiert, da sie nur zum eigenen Gebrauch der Richterin und des Richters oder allenfalls zum kammerinternen/senatsinternen Gebrauch bestimmt sind. Solche Entscheidungssammlungen sind nicht nur für die richterliche Arbeit hilfreich, sondern auch für die Einheitlichkeit und Kontinuität der Rechtsprechung unabdingbar, da der Großteil der Entscheidungen nicht veröffentlicht wird.

Auch ist zu berücksichtigen, dass regelmäßig die personenbezogenen Daten für die weitere Nutzung von gesammelten Entwürfen irrelevant sind. Für den internen Gebrauch ist die Kenntnis der Richterin oder des Richters von der Identität der Parteien in aller Regel bedeutungslos. Sie sind lediglich ein Annex zu den allein interessierenden rechtlichen Ausführungen im einheitlichen Textdokument der Entscheidung. Gleichwohl ist ihre Trennung bzw. isolierte Löschung aus den Entwürfen insbesondere bei einer rückwirkenden Bereinigung mit einem sehr hohen Arbeitsaufwand verbunden, der den betroffenen Verfahrensbeteiligten keinen Vorteil beim Datenschutz bringt. Nach den Aufbewahrungsvorschriften müssen die Akten und die abschließenden Entscheidungen ohnehin über einen längeren Zeitraum aufbewahrt werden. Über das Aktenzeichen, das zu speichern zulässig ist, kann die einzelne Richterin oder der einzelne Richter, so er denn Interesse an den Partei-

identitäten hat, jederzeit auf die aufbewahrten Akten und damit die personenbezogenen Daten zugreifen. Dass dies in der Praxis nur in absoluten Ausnahmefällen geschieht, zeigt, dass die einzelnen Richter gerade kein Interesse an den personenbezogenen Daten der Parteien haben, sondern allein an den rechtlichen Ausführungen. Hinzu kommt, dass bei konsequenter Fortführung dieser Rechtsauffassung nicht nur die Personalien aus den Entwürfen herauszulöschen oder zu schwärzen wären, sondern unter Umständen auch Teile des Tatbestandes (insbesondere aus Strafurteilen), sofern darin Daten enthalten sind, die einer bestimmten Person zugeordnet werden können. Dabei müssten im Entscheidungstext nicht einmal Namen genannt werden. Eine echte Grenzziehung ist hierbei unmöglich.

Sofern Richterinnen und Richter sich elektronische Entscheidungssammlungen halten, ist zudem die Gefahr des Missbrauchs oder der unbefugten Kenntnisnahme nicht gegeben, da nur die jeweiligen Richter selbst, auch im Falle der Vernetzung, Zugriff auf die Daten haben.

Schließlich ist wertend zu berücksichtigen, dass außer in Fällen des Ausschlusses der Öffentlichkeit die Verfahren regelmäßig in öffentlicher Verhandlung geführt werden. Es ist dabei sogar jedem Dritten möglich, deutlich mehr personenbezogene Daten als nur die Personalien der Parteien in öffentlicher Sitzung zu erfahren.

Schließlich müssen auch die begrenzten Kontrollmöglichkeiten gegenüber Richterinnen und Richtern berücksichtigt werden. Das Ministerium der Justiz könnte zwar die einzelnen Richterinnen und Richter per Erlass dazu auffordern, Anonymisierungen vorzunehmen. Im Bereich der richterlichen Unabhängigkeit ist eine Kontrolle aber nicht statthaft.

Die Landesregierung ist deshalb der Auffassung, dass hier der Rechtsgedanke des § 13 Abs. 3 HDSG herangezogen werden sollte, wonach an die Stelle der Trennungspflicht ein Verwertungsverbot dieser personenbezogenen Daten tritt, wenn sie "in Akten" derart verbunden sind, dass ihre Trennung nach verschiedenen Zwecken nur mit einem unverhältnismäßigem Aufwand möglich ist.

Dies gilt jedoch nur für interne Entscheidungssammlungen der einzelnen Richterinnen und Richter oder des Spruchkörpers. Sofern Urteile in Entscheidungssammlungen zentral in Bibliotheken eingestellt werden, ist dagegen eine Anonymisierung unabdingbar und auch zumutbar. Eine solche zentrale Entscheidungssammlung wird sich schon nach ihrem Zweck auf wenige grundlegende Entscheidungen begrenzen, sodass die Anzahl der zu anonymisierenden Dokumente niedrig ist. Andererseits besteht hier mit dem vergrößerten Kreis der Personen, die in solche Sammlungen Einsicht nehmen können, eine größere Missbrauchsgefahr.

Zu 6. Polizei- und Strafverfolgungsbehörden

Zu 6.1 Mangelnde Verwertung des Verfahrensergebnisses bei Datenspeicherungen durch die Polizei

Zu 6.1.1 Verweigerung begehrter Berichtigung

Infolge der Umorganisation der hessischen Polizei ist das Polizeipräsidium Mittelhessen in Gießen für die Bearbeitung der Angelegenheit zuständig geworden. Nach Prüfung der Akten hat die Behörde den Bescheid aufgehoben und die beantragte Löschung vorgenommen.

Die Entscheidung des Polizeipräsidioms Mittelhessen war zutreffend, denn durch die Angabe der Staatsanwaltschaft, es bestehe kein begründeter Tatverdacht mehr, waren die Voraussetzungen des § 20 Abs. 4 HSOG entfallen.

Zu 6.1.3 Unterbleibende Löschung trotz Freispruch

Die Auffassung des Datenschutzbeauftragten, ein Verdacht, der die weitere Speicherung von Daten rechtfertige, entfalle ohne weiteres bei Freispruch und vergleichbaren Verfahrenseinstellungen, wird nicht geteilt. Auf die Ausführungen zu Nr. 6.1.6 wird verwiesen.

Die vom Datenschutzbeauftragten festgestellten Mängel werden nicht in Abrede gestellt. Die Stichprobe von 13 ausgewählten Akten sollte jedoch im Zusammenhang mit den Gesamtzahlen bewertet werden. Im Jahre 2000 sind dem Polizeipräsidium Frankfurt am Main 36.275 Verfahrensausgänge von der örtlichen Staatsanwaltschaft mitgeteilt worden. Für die Auswertung ste-

hen drei bis vier besonders geschulte Mitarbeiter zur Verfügung, von denen jeder im Durchschnitt 47 Fälle pro Arbeitstag erledigt. Das Polizeipräsidium Frankfurt am Main hat die Mängel jedoch zum Anlass genommen, die Mitarbeiter erneut zu sensibilisieren und an die Notwendigkeit einer sorgfältigen Bearbeitung zu erinnern.

Zu 6.1.4 Unzureichende Sachstandsmitteilung durch die Staatsanwaltschaft

Soweit die Justiz betroffen ist, ist einzuräumen, dass die Umsetzung der früher lediglich auf der Ebene einer Verwaltungsvorschrift, nunmehr aber gesetzlich geregelten Mitteilung über den Verfahrensausgang an die Polizeibehörden (§ 482 StPO) in der Praxis verschiedentlich Probleme bereitet hat. Dem Tätigkeitsbericht ist auch beizupflichten, dass die Mitteilungspflicht der Staatsanwaltschaft unabhängig von einer formularmäßigen Anforderung durch die Polizei besteht. Dies wurde gegenüber dem Generalstaatsanwalt auch nochmals klargestellt. Die Landesregierung geht davon aus, dass den bisher in Einzelfällen auftretenden Säumnissen bei der Übermittlung des Verfahrensabschlusses durch die flächendeckende Einführung des Verfahrens MESTA bei den hessischen Staatsanwaltschaften künftig wirksam begegnet werden kann.

Nach § 482 StPO besteht die Mitteilungspflicht gegenüber "der Polizeibehörde, die mit der Angelegenheit befasst war". Die Mitteilung soll die Polizeibehörden in die Lage versetzen, die in Ihren Unterlagen vorhandenen Informationen entsprechend dem Ergebnis des Verfahrens zu bereinigen. Empfänger sind daher die Dienststellen, die auf der Seite der Polizei federführend mit der Sachbearbeitung befasst sind und daher entsprechend den KPS-Richtlinien die polizeilichen Kriminalakten führen. Eine Übermittlung an alle im Verfahren kontaktierten Polizeidienststellen, auch wenn diese nur im Rahmen einzelner Ermittlungersuchen tätig geworden sind, würde gerade in umfangreicheren Strafverfahren zu einem uferlosen Mitteilungswesen führen, das auch aus der Sicht des Datenschutzes wohl nicht günstig wäre.

Zu 6.1.5 Die Rechtslage

Die so genannten KPS-Richtlinien vom Februar 1992 sind dem neu gefassten § 20 Abs. 4 HSOG sowie der veränderten Organisationsstruktur der hessischen Polizei anzupassen. Ein entsprechender Entwurf liegt dem Datenschutzbeauftragten zur Stellungnahme vor. Die Regelung über die Behandlung von Freisprüchen und Einstellungen ist indes nicht änderungsbedürftig. Sie entstammt einem Formulierungsvorschlag, den der Datenschutzbeauftragte im Dezember 1991 unterbreitet hat. Seither hat der Gesetzgeber die Rechtslage im Sinne der Richtlinien präzisiert (vgl. zu Nr. 6.1.6).

Die KPS-Richtlinien enthalten sehr differenzierte Regelungen über die Speicherung von Strafverfahren. So führen Ermittlungsverfahren wegen Fahrlässigkeitsdelikten und wegen vorsätzlicher Verkehrsdelikte von vornherein nicht zur Aufnahme in die Kriminalpolizeilichen Sammlungen. Bei Antragsdelikten wird unterschieden nach der Art des Delikts und der Stellung eines Strafantrags bzw. der Bejahung des besonderen öffentlichen Interesses durch die Staatsanwaltschaft. Schließlich ist die Polizeibehörde gehalten, Vorgänge auszusondern, die zwar nach den sonstigen Bestimmungen der Richtlinien gespeichert werden dürften, deren Speicherung sie selbst aber nicht für erforderlich hält. Kommt es zu einer Speicherung, hängt die Aufbewahrungsdauer nach Maßgabe der Prüffristenverordnung vom Alter der betroffenen Person sowie Art und Schwere des Delikts ab.

Zu 6.1.6 Fazit

Der Auffassung des Datenschutzbeauftragten, jeder Freispruch und jede Einstellung eines Strafverfahrens durch die Staatsanwaltschaft beinhalte die "Regelvermutung, dass der Verdacht ... nicht aufrecht zu halten ist", so dass sich für den Regelfall eine Löschungspflicht ergebe, kann nicht gefolgt werden. Die Befugnis zur weiteren Speicherung fehlt nur dann, wenn der ursprüngliche Verdacht, die betroffene Person habe eine Straftat begangen (Anfangsverdacht im Sinne des § 152 Abs. 2 StPO), entfällt. Der Gesetzgeber hat dies durch das Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 3. November 1998 (GVBl. I S.399) in Abkehr von der Rechtsprechung hessischer Verwaltungsgerichte so be-

stimmt, um der Polizei auch die fortgesetzte Speicherung solcher Verfahren zu ermöglichen, die aus Mangel an Beweisen mit einer Einstellung oder einem Freispruch endeten.

Im Gegensatz zum geänderten HSOG gibt das Strafverfahrensänderungsgesetz 1999 keinen Anlass, die KPS-Richtlinien zu novellieren. Die Strafprozessordnung lässt nämlich die Verwendung von Strafverfahrensdaten nach Maßgabe der Polizeigesetze zu (§§ 481, 484 Abs.4 StPO). Dass im Falle eines Freispruches das Urteil daraufhin zu überprüfen ist, ob der Anfangsverdacht entfallen ist, ist bereits geregelt (Nr. 17.3.2 der KPS-Richtlinien).

Zu 6.2 Medienpräsenz bei behördlichen Kontrollen und polizeilich angeordneten Maßnahmen

Das Ministerium des Innern und für Sport hat den Vorschlag des Datenschutzbeauftragten aufgegriffen und die Richtlinien über Mitteilungen der Polizei an die Presse und den Rundfunk vom 21. Dezember 1999 wie folgt ergänzt (StAnz. 22/2001, S. 1906):

"2.4 Zusammenarbeit bei der Produktion von Sendungen über polizeiliche Einsätze

2.4.1 Den Wünschen von Fernseheinrichtungen, vorab über polizeiliche Einsätze unterrichtet zu werden, um diese filmen zu können (so genanntes Reality-TV), ist nur dann zu entsprechen, wenn dies, z.B. wegen der Präventionswirkung, im öffentlichen Interesse liegt und datenschutzrechtliche Belange der betroffenen Personen nicht beeinträchtigt werden.

2.4.2 Datenschutzrechtliche Belange der betroffenen Personen werden nicht beeinträchtigt, wenn die Fernseheinrichtung folgende Voraussetzungen schriftlich anerkannt hat:

- Keine Person – Bürger oder Beamter – darf aufgenommen werden, die nicht vorher nach Aufklärung über den Umfang, Zweck und Dauer der Aufnahmen ihr Einverständnis erklärt hat. Auf die Freiwilligkeit der Einwilligung ist die betroffene Person hinzuweisen.
- Solange keine Einwilligung eingeholt worden ist, weil die betroffene Person vom Aufnahmeteam noch nicht angesprochen werden konnte, dürfen nur Übersichtsaufnahmen erstellt werden, die die betroffene Person nicht klar erkennen lassen.
- Personen oder andere personenbezogene Umstände (insbesondere amtliche Kennzeichen) dürfen ohne zusätzliche schriftliche Einwilligung nicht gesendet werden. Sie sind durch Schnitt zu löschen oder unkenntlich zu machen. Personenbezogenes Aufnahmematerial ist nach der Auswertung für die Sendung zu löschen. Die Löschung ist zu dokumentieren.
- Der fertige Film ist der Polizeibehörde zur Abnahme in datenschutzrechtlicher Hinsicht so rechtzeitig vorzulegen, dass Änderungen noch vor der Sendung möglich sind. Forderungen der Polizei nach Anonymisierung von Personen oder Sachen mit Personenbezug hat die Fernseheinrichtung zu entsprechen."

Zu 6.3 Verarbeitung der Hessischen Polizeidaten beim Bundeskriminalamt im Wege der Datenverarbeitung im Auftrag

Die vom Datenschutzbeauftragten kritisierte Auftragsdatenverarbeitung beim Bundeskriminalamt wird es nicht geben. Aufgrund der Entscheidung des Ministeriums des Innern und für Sport vom 29. Dezember 2000 ist am Jahresbeginn das Projekt "POLAS Hessen" in Angriff genommen worden. Die Projektgruppe passt das bei der Hamburger Polizei eingesetzte Datenverarbeitungssystem an die hessischen Verhältnisse an. Hessen kann daher wie Hamburg auf eine Auslagerung seiner polizeilichen Datenverarbeitung zum Bundeskriminalamt verzichten.

Zu 11. Entwicklungen im Bereich der Technik
Zu 11.1 Schwachstellensuche bei Firewalls und in Rechnernetzen
Zu 11.1.2.1 Ergebnisse der Schwachstellenanalyse

Durch die Darstellung der Ergebnisse der Schwachstellenanalyse könnte der Eindruck entstehen, dass für die Informationsserver im praktischen Betrieb ein hohes Risiko bestünde. Dies ist aus Sicht der HZD nicht der Fall. Vielmehr ist festzustellen, dass die untersuchten Server in einem besonders geschützten Netzsegment betrieben werden. Dieses Segment ist zum Internet hin durch einen Paketfilter abgesichert. Die Einbruchversuche bei der Schwachstellenanalyse wurden von einem System vorgenommen, das sich innerhalb dieses geschützten Netzsegments befand. Ein potenzieller Angreifer aus dem Internet müsste sich daher zunächst Zugang zu diesem Netz verschaffen, um die festgestellten Schwachstellen ausnutzen zu können. Auf dem Paketfilter werden u.a. auch die beschriebenen Netbios-Ports gefiltert. Die dargestellten Sicherheitslücken durch Netbios-Freigaben auf den Servern bedeuten daher keine Gefahr durch Angriffe aus dem Internet.

Die Ergebnisse der Schwachstellenanalyse haben gezeigt, dass das im HCN 2000 umgesetzte Sicherheitskonzept ein hohes Maß an Schutz gewährleistet.

Zu 12. Ausländerrecht
Zu 12.2 Kontrolle der Ausländerbehörde des Rheingau-Taunus-Kreises
Zu 12.2.1 Verfahren bei der Ermittlung von so genannten Scheinehen

Der Datenschutzbeauftragte bedauert, dass ihm das Ministerium des Innern und für Sport im Sommer 2000 mitgeteilt habe, keinen Erlass zur Ermittlung von Scheinehen zu fertigen, nennt aber nicht die Gründe, die ihm das Ministerium für seine Entscheidung dargelegt hat.

Die Anregung des Datenschutzbeauftragten, den Ausländerbehörden durch Erlass die wesentlichen Rechtmäßigkeitsvoraussetzungen für die Ermittlung von Scheinehen an die Hand zu geben, führte zu einer eingehenden Prüfung der Frage, welche Regelungen in einen solchen Erlass aufzunehmen wären und welche Folgen sich daraus für die Verwaltungspraxis ergäben. In diese Prüfung hat das Ministerium des Innern und für Sport eine Reihe nachgeordneter Behörden einbezogen, um deren Erfahrungen in dem Erlass berücksichtigen zu können. Die Berichte der beteiligten Ausländerbehörden zeigten die Problematik einer solchen Regelung auf.

Zum einen würde der Erlass nur allgemeine Verfahrensregelungen treffen, die naturgemäß nicht allen Fallgestaltungen gerecht werden können. Nicht nur die Umstände, die den Verdacht auf Bestehen einer Scheinehe begründen, sind individuell sehr verschieden, sondern auch die Bearbeitungsmöglichkeiten der Ausländerbehörden. Die angemessene Beachtung der höchst unterschiedlichen Anforderungen der Praxis wäre deshalb in einem generellen Erlass nicht möglich gewesen. Die Bindung an abstrakte Regelungen, die den Besonderheiten des Einzelfalles nicht gerecht werden, würde jedoch zu einer erheblichen Beeinträchtigung der Arbeit der Ausländerbehörden führen. Dieser Beeinträchtigung stünde kein sicherer Gewinn in Form eines verbesserten Schutzes der personenbezogenen Daten der Betroffenen gegenüber. Auch dies haben die Berichte der Ausländerbehörden verdeutlicht, die teilweise ausführlich auf die datenschutzrechtlichen Gesichtspunkte eingingen und dadurch das vorhandene Problembewusstsein der Mitarbeiterinnen und Mitarbeiter der Ausländerbehörden belegen.

Das Ministerium des Innern und für Sport hat sich deshalb gegen eine allgemeine Verfahrensanleitung für alle Ausländerbehörden entschieden. Eine solche Regelung würde lediglich zur Bürokratisierung des Verwaltungsvorganges führen, ohne dafür einen Zuwachs im Bereich des Datenschutzes zu erhalten. Dies widerspräche auch dem Ziel der Landesregierung, die Verwaltung von der Last unnötiger Vorschriften zu befreien und dadurch effizienter zu machen. Sofern zukünftig bei einer Stelle vorhandene Defizite erkannt werden, sollen diese durch gezielte Hinweise im Einzelfall behoben werden. Außerdem wurde bzw. wird die Thematik im Rahmen der turnusmäßig stattfindenden Dienstbesprechungen mit den Ausländerbehörden erörtert.

Zu 13. Melderecht

Zu 13.2 Datenübermittlungen der Einwohnermeldeämter an die Gebühreneinzugszentrale

Das DV-technische Problem beim Zuzug eines allein stehenden Minderjährigen zu einer Familie wird mit dem KIV/dem KGRZ erörtert werden, um ähnliche Probleme für die Zukunft auszuschließen. Rechtliche Hindernisse stehen einer Datenübermittlung an die GEZ nicht entgegen. § 34 Abs. 7 HMG, der ein Auskunftsverbot für die Fälle der Anbahnung einer Adoption vorsieht, gilt für die öffentlich-rechtlichen Rundfunkanstalten nur, soweit sie publizistische Tätigkeiten ausüben (§ 34 Abs. 8 HMG).

Wiesbaden, 21. August 2001

Der Hessische Ministerpräsident
Koch

Der Hessische Minister des Innern
und für Sport
Bouffier