

## **4. Tätigkeitsbericht**

der Beauftragten für den Datenschutz  
des Rundfunk Berlin-Brandenburg

### **Berichtszeitraum:**

1. April 2006 bis 31. März 2007

Dem Rundfunkrat gemäß § 38 Abs. 7 **rbb**-Staatsvertrag  
vorgelegt von Anke Naujock

Inhaltsverzeichnis
--------------------

	<u>Seite</u>
Vorbemerkung	4
<b>A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg</b>	5
I.    Gesetzliche Grundlagen	5
II.   Konkrete Situation	6
III.  Zusammenarbeit mit anderen Stellen im <b>rbb</b>	6
<b>B. Entwicklung des Datenschutzrechts</b>	7
I.    Gesetzgebung	7
1.    Änderung des Bundesdatenschutzgesetzes	7
2.    9. Rundfunkänderungsstaatsvertrag/ Telemediengesetz – TMG	9
3.    10. Rundfunkänderungsstaatsvertrag	9
4.    Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums	12
5.    Allgemeines Gleichbehandlungsgesetz	13
II.   Rechtsprechung	14
1.    Entscheidung des Europäischen Gerichtshofs zur Übermittlung von Fluggastdaten	14
2.    Verletzung der Pressefreiheit durch Durchsuchung und Beschlagnahme bei Presseredaktionen (BVerfG, Urteil vom 27.2.2007)	15
3.    Online-Archive	16
<b>C. Datenschutz und Datensicherheit im rbb</b>	17
I.    Aktuelle IT-Projekte	17
1.    RMS	18
2.    Neues Dispositionssystem im <b>rbb</b>	18
3.    Ersatz des Online Content Management Systems (CMS)	19
4.    Bewerbermanagementsystem	20

	<u>Seite</u>
II. Organisatorische Regelungen	20
1. Dienstvereinbarung über die Einführung und Anwendung des Telekommunikationsanlagenverbundes	20
2. Dienstvereinbarung über die Nutzung mobiler Telekommunikationsgeräte	22
3. Richtlinien für den Einsatz von Externen bei der Wartung von IT- und TK-Systemen	22
III. Sonstiges	24
1. Stasi-Überprüfung im <b>rbb</b>	24
2. Diverse Einzelvorgänge	25
IV. Schulungen	26
<b>D. Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung</b>	<b>26</b>
I. Allgemeines	26
II. GEZ	30
1. Konsolidierungsarbeiten zum Projekt DV2005	30
2. Neues Löschkonzept	31
3. Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Bremen, Hessen, Berlin und Brandenburg	32
4. Verfahren bei der Befreiung von der Rundfunkgebühr	32
5. NP-Datenbank	34
III. Rundfunkgebührenabteilung	35
<b>E. Datenschutz im Informationsverarbeitungszentrum (IVZ)</b>	<b>35</b>
I. Allgemeines	35
II. Einzelne Themen	36
1. BSI-Zertifizierung	36
2. Dokumentenmanagement im IVZ	36
3. Telearbeitsplätze	37
III. Organisatorische Regelungen	38
<b>F. Datenschutz im ARD-Hauptstadtstudio (HSB)</b>	<b>38</b>
<b>G. Sonstiges</b>	<b>39</b>
I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR	39
II. IT-Sicherheitsgremium für das ARD-Corporate Network	40
III. Teilnahme an Veranstaltungen	41

## Vorbemerkung

Dieser Tätigkeitsbericht soll einen Überblick über meine Aktivitäten als Datenschutzbeauftragte des **rbb** in dem Zeitraum 1. April 2006 bis 31. März 2007 geben. Er umfasst sowohl meine Tätigkeit als Datenschutzbeauftragte für den journalistisch-redaktionellen Bereich gemäß § 38 **rbb**-Staatsvertrag, als auch meine Betätigung als sog. behördliche Datenschutzbeauftragte gemäß § 19a Berliner Datenschutzgesetz (BerIDSG). Trotz des im letzten Jahr von einem Mitglied des Rundfunkrates geäußerten Wunsches nach einer anderen Gliederung, halte ich an der bislang in allen meinen bisherigen Tätigkeitsberichten gewählten Reihenfolge fest. Sie entspricht im Wesentlichen auch derjenigen, die die Rundfunkdatenschutzbeauftragten der anderen Häuser einhalten und gewährleistet dadurch eine schnelle Orientierung.

Der Anforderung des Artikel 28 Absatz 5 EU-Datenschutzrichtlinie, wonach jede unabhängige, den Datenschutz kontrollierende Stelle verpflichtet ist, ihre Tätigkeitsberichte zu veröffentlichen, komme ich durch Veröffentlichung meiner Berichte auf der Website des **rbb** im Internet nach.

Der Abruf kann über

*[http://www.rbb-online.de/\\_/unternehmen/index\\_jsp/activeid=2312.html](http://www.rbb-online.de/_/unternehmen/index_jsp/activeid=2312.html)*

erfolgen. Dort finden sich bereits die Berichte aus den Jahren 2003 bis 2006.

Förmliche Beanstandungen habe ich im Berichtszeitraum nicht ausgesprochen. Soweit es in Einzelfällen zu Verletzungen von Datenschutzbestimmungen gekommen ist, wurde meinen Empfehlungen in den Fachbereichen umgehend gefolgt und die datenschutzrechtliche Verletzung abgestellt.

Insgesamt lässt sich festhalten, dass der Datenschutz im Bewusstsein der **rbb**-Mitarbeiterinnen und -Mitarbeiter sehr ausgeprägt ist. Dies belegen u. a. die vielen Anfragen, die rein präventiv an mich gerichtet werden.

## A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg

### I. Gesetzliche Grundlagen

Die Rechtsgrundlagen für die Tätigkeit der Datenschutzbeauftragten des **rbb** haben sich im Berichtszeitraum nicht verändert.

Gemäß § 38 Abs. 1 **rbb**-Staatsvertrag bestellt der Rundfunkrat einen Beauftragten oder eine Beauftragte für den Datenschutz. Der oder die Beauftragte für den Datenschutz ist in Ausübung seines/ihrer Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er/sie der Dienstaufsicht des Verwaltungsrates.

Gemäß Abs. 2 Satz 2 überwacht er/sie die Einhaltung der Datenschutzvorschriften des **rbb**-Staatsvertrags und anderer Vorschriften über den Datenschutz, soweit der **rbb** personenbezogene Daten zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet.

Soweit eine Befugnis des oder der Beauftragten für den Datenschutz nach Abs. 2 Satz 1 nicht gegeben ist, obliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen beim **rbb** dem oder der Landesbeauftragten für den Datenschutz des Landes Berlin. Die Kontrolle erfolgt im Benehmen mit dem oder der Landesbeauftragten des Datenschutzes des anderen Landes (Abs. 8).

Die Rundfunkdatenschutzbeauftragte ist eine eigenständige Kontrollstelle im Sinne von Artikel 28 EG-Datenschutzrichtlinie.

Für die Sicherstellung des Datenschutzes im wirtschaftlich-administrativen Bereich ist beim **rbb** außerdem – wie bei allen Berliner Behörden und sonstigen öffentlich-rechtlichen Stellen – eine behördliche/ein behördlicher Datenschutzbeauftragte/r sowie jeweils eine Stellvertreterin/ein Stellvertreter schriftlich zu bestellen (§ 36 Abs. 1 **rbb**-Staatsvertrag i. V. m. § 19 a Berliner Datenschutzgesetz –BlnDSG).

## II. Konkrete Situation

Auf seiner Sitzung am 26. Mai 2003 hat mich der Rundfunkrat gemäß § 38 Abs. 1 **rbb**-Staatsvertrag auf Vorschlag der Intendantin für eine Amtszeit von vier Jahren zur Beauftragten für den Datenschutz des **rbb** gewählt. Parallel dazu hat mich die Intendantin für den gleichen Zeitraum mit der Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten im Sinne von § 19a BlnDSG beauftragt. Eine Stellvertretung für die behördliche Datenschutzbeauftragte ist noch nicht bestellt. Meine Funktion als Datenschutzbeauftragte des **rbb** nehme ich nebenamtlich zu meiner Tätigkeit im Justitiariat wahr.

Die Befassung mit datenschutzrechtlichen Themen im **rbb** durch die Datenschutzbeauftragte des Landes Brandenburg, Frau Dagmar Hardtke, und den Berliner Landesdatenschutzbeauftragten, Herrn Dr. Alexander Dix, beschränkte sich auch im Berichtszeitraum wieder auf den Bereich der Rundfunkteilnehmerdatenverarbeitung. In vielen Fragestellungen gibt es erfreuliche inhaltliche Übereinstimmungen in der datenschutzrechtlichen Bewertung zwischen den staatlichen Datenschutzbeauftragten und mir, die ein gemeinsames Vorgehen in der Sache ermöglichen.

Diese positiven praktischen Erfahrungen ändern freilich nichts an meinem Rechtsstandpunkt, wonach die Übertragung der Kontrollkompetenzen im wirtschaftlich-administrativen Bereich auf die staatlichen Datenschutzbeauftragten, die es vergleichbar außer beim **rbb** nur noch beim Hessischen Rundfunk und bei Radio Bremen gibt, verfassungsrechtlich zumindest bedenklich ist.

## III. Zusammenarbeit mit anderen Stellen im rbb

Auch im vergangenen Jahr habe ich wieder sehr eng mit dem IT-Sicherheitsbeauftragten, Herrn Gerry Wolff, zusammengearbeitet.

Insbesondere bei der datensicherheitstechnischen Bewertung von IT-Systemen im Rahmen der Vorabkontrolle gemäß § 19 a Ziff. 1 BerlDSB i. V. m. § 31 Abs. 5 der Geschäftsordnung des **rbb** bin ich auf die Zusammenarbeit mit Herrn Wolff ange-

wiesen. Die Einzelheiten des bei der Vorabkontrolle einzuhaltenden Verfahrens sind in Ziffer 5 der Datenschutz-Dienstanweisung geregelt.

Herr Wolff steht mir als Berater in Fragen der IT-Sicherheit zeitlich leider nur eingeschränkt zur Verfügung. Als Systemverantwortlicher für IT-Sicherheit ist er für die Planung, den Betrieb und die Weiterentwicklung der IT-Sicherheits-Hard- und Software-Systeme zuständig. Aus meiner Sicht wäre es wünschenswert, Herrn Wolff mehr Arbeitszeit für seine wichtigen Aufgaben im Zusammenhang mit der datenschutzrechtlichen Vorabkontrolle von IT-Systemen einzuräumen.

Neben der Datenschutzbeauftragten hat auch der Personalrat die Aufgabe, für die Einhaltung des Datenschutzes bei der Einführung und Anwendung neuer IT-Systeme zu sorgen. Mit ihm stimme ich mich jeweils eng ab.

## **B. Entwicklung des Datenschutzrechts**

### **I. Gesetzgebung**

#### **1. Änderung des Bundesdatenschutzgesetzes**

Im August 2006 trat das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere der mittelständischen Wirtschaft in Kraft (BGBl. 1970 ff.), mit dessen Art. 1 das Bundesdatenschutzgesetz (BDSG) geändert wurde. Die Neuregelungen bewirken für die Praxis des Datenschutzes zahlreiche Änderungen, die sich hauptsächlich auf die Bestellung und die Tätigkeit der betrieblichen Datenschutzbeauftragten auswirken.

Die wichtigsten Neuerungen:

- ✍ Der sog. Beschäftigten-Schwellenwert als Kriterium für die Pflicht zur Bestellung eines/einer betrieblichen Datenschutzbeauftragten wurde von 5 auf 10 Personen hoch gesetzt (§ 4 f Abs. 1).

- ✍ Unter Bezugnahme auf den Umfang und den Schutzbedarf der verarbeiteten Daten wurde der bisher gesetzlich nicht näher bestimmte Begriff der Fachkunde präzisiert. Danach bestimmt sich das Maß der erforderlichen Fachkunde des/der betrieblichen Datenschutzbeauftragten insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet (§ 4 f Abs. 2).
- ✍ Klargestellt wurde, dass sich die Pflicht zur Bestellung eines/einer betrieblichen Datenschutzbeauftragten auch auf sog. Berufsgeheimnisträger (Rechtsanwälte, Ärzte, Apotheker, Steuerberater etc.) bezieht (§ 4f Abs. 2). Für die Datenschutzbeauftragten gelten die entsprechenden Zeugnisverweigerungsrechte analog.
- ✍ Den betrieblichen Datenschutzbeauftragten wurde ein gesetzlicher Beratungsanspruch gegenüber den Aufsichtsbehörden eingeräumt (§ 38 Abs. 1)

Der **rbb** wird von diesen Neuregelungen nicht unmittelbar tangiert. Für ihn gelten in erster Linie die Spezialregelungen zum Datenschutz des **rbb**-Staatsvertrages und ergänzend die Regelungen des Berliner Datenschutzgesetzes (§ 36 Abs. 1 **rbb**-Staatsvertrag).

Allerdings sind die Regelungen des BDSG für die Beteiligungsgesellschaften des **rbb** relevant. Da es sich um privatrechtliche Gesellschaften handelt, findet auf diese grundsätzlich das BDSG Anwendung. In Einzelfällen berate ich auch die Beteiligungsgesellschaften des **rbb** in datenschutzrechtlichen Angelegenheiten. So war ich beispielsweise im Frühjahr 2007 mit Fragen der datenschutzrechtlichen Zulässigkeit der Installation einer Webcam durch eine Tochtergesellschaft des **rbb** auf einem Hotel am Alexanderplatz befasst, mit der Bilder als Livestream im Internet übertragen werden.

## **2. 9. Rundfunkänderungsstaatsvertrag/Telemediengesetz - TMG**

Am 10. Oktober 2006 haben die Regierungschefs der Länder den Neunten Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (9. Rundfunkänderungsstaatsvertrag) unterzeichnet.

Die Änderungen betreffen den Rundfunkstaatsvertrag, den Jugendmedienschutz-Staatsvertrag, den ARD-Staatsvertrag, den ZDF-Staatsvertrag, den Deutschlandradio-Staatsvertrag, den Rundfunkgebührenstaatsvertrag, den Rundfunkfinanzierungsstaatsvertrag und die Aufhebung des Mediendienste-Staatsvertrags.

Schwerpunkt der Änderungen ist die Fortführung der Reform des Medienrechts zwischen Bund und Ländern durch Anpassung und Vereinheitlichung der bereichsspezifischen Regelungen für Teledienste und Mediendienste. Unter dem einheitlichen Begriff „Telemedien“ werden Teledienste und Mediendienste nun zusammengefasst. Die wirtschaftsbezogenen Bestimmungen für Telemedien (Herkunftslandprinzip, Zulassungsfreiheit, Informationspflichten, Verantwortlichkeit, Datenschutz) sind jetzt im Telemediendienstgesetz (TMG) des Bundes enthalten, das zeitgleich mit dem 9. Rundfunkänderungsstaatsvertrag in Kraft getreten ist. Die über die wirtschaftsrechtlichen und allgemeinen Anforderungen hinausgehenden inhaltespezifischen Regelungen für Telemedien sind dagegen im Rundfunkstaatsvertrag enthalten.

## **3. 10. Rundfunkänderungsstaatsvertrag**

Derzeit wird bereits der Zehnte Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (10. Rundfunkänderungsstaatsvertrag) vorbereitet. Am 3. Mai 2006 fand eine gemeinsame Besprechung von Vertretern der Landesdatenschutzbeauftragten, der Staatskanzleien, der Rundfunkanstalten und der Rundfunkdatenschutzbeauftragten bei der GEZ in Köln statt. Dort haben sich alle beteiligten Seiten zu § 6 Abs. 2 (Nachweis der Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht) und zu § 8 Abs. 4 (Ermächtigungsgrundlage für die Anmietung von Adressen für die sog. Mailingaktionen der GEZ) Rundfunkgebührenstaatsver-

trag (RGebStV) auf einen neuen Wortlaut geeinigt. Die Umsetzung wird voraussichtlich im 10. Rundfunkänderungsstaatsvertrag erfolgen.

Zur Problematik des mit dem 8. Rundfunkänderungsstaatsvertrag am 1.4.2005 in Kraft getretenen § 6 Abs. 2 RGebStV verweise ich auf meine Ausführungen in D II 4. Die neue Fassung von § 6 Abs. 2 wird voraussichtlich folgenden Wortlaut haben:

*„Der Antragsteller hat die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht durch Vorlage einer entsprechenden Bestätigung des Leistungsträgers im Original oder die Vorlage des entsprechenden Bescheides im Original oder in beglaubigter Kopie nachzuweisen.“*

Neu ist die ausdrücklich geregelte Möglichkeit der Vorlage einer sog. Drittbescheinigung. Diese Neuregelung ist sicherlich ein Schritt in die richtige Richtung. Andererseits ist die Drittbescheinigung nach dieser Regelung aber nicht zwingend, so dass Rundfunkteilnehmer, die nicht auf eine kooperationswillige Behörde stoßen, sich nach wie vor in einem datenschutzrechtlichen Dilemma befinden werden, aus dem sie sich letztendlich nur durch Schwärzungen in den beglaubigten Kopien befreien können. Laut GEZ gibt es mit den Schwärzungen in der Praxis zahlreiche Probleme. Häufig werden Angaben geschwärzt, die für die Frage der Befreiungsfähigkeit relevant sind. Dem extrem hohen Verwaltungsaufwand bei der GEZ wird diese Neuregelung folglich nur bedingt entgegen wirken.

Mit dem 8. Rundfunkänderungsstaatsvertrages ist § 8 Abs. 4 in den Rundfunkgebührenstaatsvertrag aufgenommen worden, der als klarstellende Rechtsgrundlage für die Anmietung von Adressen für die Mailing-Aktionen der GEZ gedacht war. In meinen früheren Tätigkeitsberichten bin ich bereits darauf eingegangen, dass diese Vorschrift von einigen Landesdatenschutzbeauftragten als zu unbestimmt und weit kritisiert wird. Der rbb hält in Übereinstimmung mit seiner Rechtsaufsicht daran fest, dass § 8 Abs. 4 RGebStV in seiner aktuellen Fassung eine geeignete Rechtsgrundlage für die Anmietung der Adressen durch die GEZ für die Mailing-Briefe ist. Andererseits begrüßt er den jetzt gefundenen Kompromiss. Danach soll § 8 Abs. 4 wie folgt neu gefasst werden:

*„Die zuständige Landesrundfunkanstalt oder die von ihr beauftragte Stelle nach Absatz 2 kann zur Feststellung, ob ein den Vorschriften dieses Staatsvertrages genügendes Rundfunkteilnehmerverhältnis besteht, und zur Verwaltung von Rundfunkteilnehmerverhältnissen personenbezogene Daten bei nichtöffentlichen Stellen ohne Kenntnis des Betroffenen erheben, verarbeiten oder nutzen. Voraussetzung dafür ist, dass*

1. *die Datenbestände dazu geeignet sind, Rückschlüsse auf die Gebührenpflicht zuzulassen, insbesondere durch Abgleich mit dem Bestand der nach § 3 angemeldeten Rundfunkteilnehmer und*
2. *sich die Daten auf Angaben zu*
  - a) *Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe*
  - b) *Berufs-, Branchen- oder Geschäftsbezeichnungen*
  - c) *Vor- und Familiennamen*
  - d) *Titel*
  - e) *Anschrift und*
  - f) *Geburtsdatum*

*beschränken und kein erkennbarer Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung Verarbeitung oder Nutzung hat. Es dürfen keine Daten, die Rückschlüsse auf tatsächliche oder persönliche Verhältnisse liefern könnten, an die übermittelnde Stelle rückübermittelt werden. Die Daten sind spätestens zwölf Monate nach ihrer Erhebung zu löschen. Sie sind unverzüglich zu löschen bei Feststellung des Nichtbestehens oder des Bestehens eines Rundfunkteilnehmerverhältnisses, das den Voraussetzungen dieses Staatsvertrages entspricht.“*

An Änderungen ist insbesondere hervorzuheben, dass der Katalog der Daten, die zum Zwecke der Feststellung eines Rundfunkteilnehmerverhältnisses und zur Verwaltung der Rundfunkteilnehmerverhältnisse erhoben werden dürfen, jetzt abschließend in der Vorschrift geregelt sein wird. Die Zulässigkeit der Datenverarbeitung wird von der Geeignetheit der Daten abhängig gemacht. Daten, die Rückschlüsse auf tatsächliche oder persönliche Verhältnisse liefern können, dürfen zu-

künftig nicht mehr an die übermittelnde Stelle zurück übermittelt werden – auch nicht zur Geltendmachung von Gewährleistungsansprüchen (wie bislang üblich). Außerdem soll festgelegt werden, dass die Daten spätestens zwölf Monate nach ihrer Erhebung zu löschen sind.

#### **4. Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums**

Am 24. Januar 2007 hat die Bundesregierung den Entwurf eines Gesetzes zur Umsetzung der EU-Richtlinie 2004/48/EG des Europäischen Parlamentes und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums beschlossen. Der Bundestag hat am 26. April 2007 über den Gesetzentwurf der Bundesregierung in erster Lesung beraten und den Gesetzesentwurf (Drucksache 16/5048) federführend dem Rechtsausschuss und dem Ausschuss für Wirtschaft und Technologie sowie nachträglich am 24. Mai 2007 dem Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz zur Mitberatung überwiesen.

Das Gesetz soll das geistige Eigentum stärken und die EU-Richtlinie durch eine Novellierung von mehreren Gesetzen zum Schutz des geistigen Eigentums umsetzen: Patengesetz, Gebrauchsmustergesetz, Markengesetz, Halbleiterschutzgesetz, Urheberrechtsgesetz, Sortenschutzgesetz werden weitgehend wortgleich geändert. Künftig soll der Kläger auch gegen Dritte – beispielsweise Internet-Provider oder Spediteure – unter bestimmten Voraussetzungen einen Auskunftsanspruch haben, um den Rechtsverletzer mit zivilrechtlichen Mitteln ermitteln zu können und seine Rechte gerichtlich besser durchsetzen zu können. Der Auskunftsanspruch soll im Einklang mit der Richtlinie aber nur dann bestehen, wenn auch die zugrunde liegende Rechtsverletzung im geschäftlichen Verkehr begangen wurde.

Ferner sollen bei einfachen Fällen mit einer nur unerheblichen Rechtsverletzung außerhalb des geschäftlichen Verkehrs die erstattungsfähigen Anwaltsgebühren für die Abmahnung nicht mehr als 50 Euro betragen. Außerdem soll im Einklang mit der bisherigen Rechtsprechung klargestellt werden, dass auch eine angemessene fiktive Lizenzgebühr als Grundlage für die Berechnung von Schadensersatz dienen könne.

Darüber hinaus wird es Erleichterungen bei der Beweisführung und ein vereinfachtes Verfahren zur Vernichtung von Piraterieware geben.

Aus datenschutzrechtlicher Sicht spielt der vorgesehene gesetzliche Auskunftsanspruch eine entscheidende Rolle. Damit wird erstmals das Fernmeldegeheimnis auch zugunsten privater wirtschaftlicher Interessen eingeschränkt. Der von der Bundesregierung geforderte Richtervorbehalt für die Herausgabe von Verkehrsdaten wurde vom Bundesrat als entbehrlich angesehen. Aus datenschutzrechtlicher Sicht scheint ein Richtervorbehalt aber unerlässlich, da die Verkehrsdaten dem Fernmeldegeheimnis unterliegen.

## **5. Allgemeines Gleichbehandlungsgesetz**

Nach einem langen und wechselhaften Gesetzgebungsverfahren ist am 18. 8. 2006 das Allgemeine Gleichbehandlungsgesetz (AGG) in Kraft getreten. Das Gesetz verbietet Diskriminierungen wegen der Rasse, der ethnischen Herkunft, des Geschlechts, der Religion, der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität. Dieser Schutz vor Diskriminierungen erstreckt sich auf das gesamte Arbeitsleben – vom Anbahnungsverhältnis bis zur Beendigung. Aus Sicht der Datenschutzbeauftragten ergeben sich wichtige Konsequenzen: Im Auswahlprozess neuer Mitarbeiter/innen ist darauf zu achten, dass keine Daten von den Bewerberinnen und Bewerbern erhoben werden, die zu einer Diskriminierung führen können. Um sich gegen einen etwaigen Verstoß gegen das Benachteiligungsverbot zu verteidigen zu können, ist für den Arbeitgeber eine Erstellung und Aufbewahrung einer Dokumentation über das Bewerbungsverfahren erforderlich. Eine solche Dokumentation berührt das informationelle Selbstbestimmungsrecht der Bewerberinnen und Bewerber. Zwar müssen Schadensersatz- oder Entschädigungsansprüche aus § 15 Abs. 1 und 2 AGG gemäß § 15 Abs. 4 AGG innerhalb einer Zwei-Monatsfrist geltend gemacht werden. Schadensersatzansprüche aus anderem Grund – insbesondere deliktische und vertragliche Ansprüche – bleiben jedoch von den Regelungen des AGG unberührt, sodass eine Aufbewahrung der Dokumentation bis zum Ablauf der allgemeinen Verjährungsfrist von drei Jahren geboten ist. Allerdings sind die Daten ab dem Zeitpunkt der Einstellungsentscheidung für den routinemä-

Bigen Zugriff durch die Sachbearbeiterinnen und Sachbearbeiter in der Personalabteilung zu sperren. Die Bewerberinnen und Bewerber müssen über die Speicherdauer unterrichtet werden. Auf diese Aspekte habe ich die Personalabteilung hingewiesen.

## **II. Rechtsprechung**

### **1. Entscheidung des Europäischen Gerichtshofs zur Übermittlung von Fluggastdaten**

Die aufgrund der Anti-Terror-Gesetzgebung der USA seit 2004 erfolgende Übermittlung von Fluggastdaten in die USA wurde vom Europäischen Gerichtshof (EuGH) für rechtswidrig befunden. Der Gerichtshof hat den zugrunde liegenden Beschluss des Rates über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und den USA sowie die Entscheidung der Europäischen Kommission über die Angemessenheit des Schutzes der personenbezogenen Daten in den Passenger Name Records (PNR) für nichtig erklärt (Urt. vom 30. 5. 2006, NJW-RR 2029).

Allerdings wurde mit dieser Entscheidung nur ein Scheinsieg für den Datenschutz errungen. Denn das Gericht hat sich nicht mit den vom Europäischen Parlament und der Art. 29-Datenschutzgruppe vorgebrachten inhaltlichen Einwänden auseinandergesetzt, sondern allein mit der formellen Frage, ob der EG-Vertrag i. V. m. der Europäischen Datenschutzrichtlinie 95/46/EG eine ausreichende rechtliche Basis für die Entscheidungen von Kommission und Rat enthält. Das hat der Gerichtshof verneint. Entsprechend der Entscheidung des EuGH galt die für nichtig erklärte rechtliche Grundlagen übergangsweise bis Ende September 2006 weiter. Am 6. 10. 2006 hat die Europäische Union mit den USA ein Zwischenabkommen vereinbart, das die Datenübermittlung in die USA sogar noch erleichtert. Das neue Abkommen gilt zunächst bis Ende Juli 2007.

## **2. Verletzung der Pressefreiheit durch Durchsuchung und Beschlagnahme bei Presseredaktionen (BVerfG, Urteil vom 27.2.2007)**

Das Bundesverfassungsgericht hat mit seinem Urteil vom 27. 2. 2007 die Durchsuchung und Beschlagnahme in den Redaktionsräumen des Magazins „Cicero“ für verfassungswidrig erklärt. Durch dieses Grundsatzurteil ist die Pressefreiheit gestärkt worden. In der Frage der Anwendbarkeit von § 353b Strafgesetzbuch (StGB; „Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht“) in der Form der Beihilfe durch Veröffentlichung vertraulicher Unterlagen durch die Journalistinnen und Journalisten gibt es jetzt mehr Rechtssicherheit.

Das Bundesverfassungsgericht ist - kurz zusammengefasst – zu folgenden Ergebnissen gekommen:

Die Anordnung der Durchsuchung der Redaktionsräume von „Cicero“ und die Beschlagnahme der dort aufgefundenen Beweismittel stellen einen verfassungsrechtlich nicht gerechtfertigten Eingriff in die Pressefreiheit des Beschwerde führenden Chefredakteurs dar. Die bloße Veröffentlichung eines Dienstgeheimnisses in der Presse durch einen Journalisten reicht nicht aus, um einen zu einer Durchsuchung und Beschlagnahme ermächtigenden Verdacht der Beihilfe des Journalisten zum Geheimnisverrat zu begründen. Erforderlich sind vielmehr spezifische tatsächliche Anhaltspunkte für das Vorliegen einer von einem Geheimnisträger bezweckten Veröffentlichung des Geheimnisses und damit einer beihilfefähigen Haupttat. Will ein Geheimnisträger einem Journalisten nur Hintergrundinformationen liefern und erfolgt die Veröffentlichung abredewidrig, ist die Tat mit der Offenbarung des Geheimnisses bereits beendet; dann kann eine Beihilfe durch die nachfolgende Veröffentlichung gar nicht mehr geleistet werden. In solchen Fällen kann eine Durchsuchung und Beschlagnahme nicht mit dem Ziel der Aufklärung einer Beihilfehandlung der Journalisten angeordnet werden. Das vollständige Urteil des Bundesverfassungsgerichts ist im Internet unter [www.bundesverfassungsgericht.de](http://www.bundesverfassungsgericht.de) veröffentlicht.

### 3. Online-Archive

Da der rbb - wie viele andere Medienunternehmen - einen Teil seiner Sendungen in einem sog. Online-Archiv auf seiner Website archiviert, stellt sich die Frage, ob eine nachträgliche Löschungspflicht hinsichtlich veröffentlichter Namen und Personenfotos wegen Zeitablaufs entstehen kann.

Nach der in der Rechtsprechung überwiegend vertretenen Auffassung (KG Berlin, AfP 2006, 506 ff.; OLG Frankfurt, AfP 2006, 569 ff.; a. A. OLG Hamburg, MMR 2007,377 f). ist dies nicht der Fall.

Nach Auffassung der Gerichte wird allein durch die Bereithaltung eines zu einem früheren Zeitpunkt erschienenen, zulässigen Beitrags in einem Archiv der Betroffene nicht erneut „an das Licht der Öffentlichkeit gezerrt“, da sich der Äußerungsgehalt lediglich in einem Hinweis auf eine in der Vergangenheit zulässige Berichterstattung erschöpfe. Dies gelte umso mehr, als der Artikel nicht ohne weiteres zugänglich ist. Der interessierte Nutzer müsse vielmehr konkret danach suchen – sei es über die Suchfunktion auf der Homepage des entsprechenden Medienunternehmens oder über eine Suchmaschine. Dabei spiele es keine Rolle, dass das Archiv nicht in Papierform, sondern elektronisch geführt wird. Zwar mag letzteres für den Nutzer schneller greifbar sein; dies sei aber allein die Folge der technischen Weiterentwicklung und könne nicht dazu führen, elektronische Archive zu untersagen. (...). Für die Unangreifbarkeit des Archivs streite das Grundrecht auf Informationsfreiheit nach Art. 5 Abs. 1 Satz 1 GG. Danach hat jeder das Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Diese Quellen dürfen jedoch nicht dadurch verändert werden, dass eine ursprünglich zulässige Berichterstattung nachträglich gelöscht werde. Dies würde zudem zu einer Verfälschung der historischen Abbildung führen und der besonderen Bedeutung von Archiven nicht gerecht werden. Im übrigen könne auch im Hinblick auf die wirtschaftliche Tragweite und den personellen und zeitlichen Aufwand für die Archivverwaltung von der Presse nicht ernsthaft verlangt werden, dass sie turnusmäßig ihre Archive daraufhin durchforstet, ob ursprünglich zulässige Berichterstattung nunmehr quasi durch Zeitablauf wegen des Anonymitätsinteresses zu sperren sei.

Ungeachtet der inzwischen ergangenen Urteile hält der **rbb** – nicht zuletzt aus Kapazitätsgründen - an seinem Archivierungskonzept aus dem Jahr 2005 fest. Danach werden Beiträge aktueller Magazine maximal 6 Wochen, jede weitere Archivierung im Rahmen der Programmbegleitung maximal 6 Monate und nur besonders ausgewählte Sendungen für einen längeren Zeitraum als 6 Monate aufbewahrt. Außerdem kommt ein sog. elektronisches Wiedervorlage-System zur Anwendung. Beiträge, die in Zukunft kritisch werden können, werden von vornherein mit einem elektronischen Textmarker versehen und auf diese Weise ggf. einer nachträglichen Prüfung unterzogen.

## **C. Datenschutz und Datensicherheit im rbb**

### **I. Aktuelle IT-Projekte**

Jede Entscheidung über den Einsatz oder die Änderung von automatisierten Systemen, mit denen personenbezogene Daten verarbeitet werden, setzt die Erarbeitung eines Sicherheitskonzepts zur Gewährleistung von Datenschutz und Datensicherheit durch die für den Betrieb der Rechnersysteme zuständige Abteilung voraus. Systeme, mit denen Personaldaten verarbeitet werden, oder die technisch dazu geeignet sind, eine Leistungs- und Verhaltenskontrolle zu ermöglichen, dürfen erst nach einer Vorabkontrolle durch die Datenschutzbeauftragten eingeführt werden (Ziffer 5.1 der Datenschutz-Dienstanweisung). Bei der Vorabkontrolle gilt es, konsequent dem Grundsatz der Datensparsamkeit Rechnung zu tragen. Das gilt auch für die Frage der Zugriffsberechtigungen und der Aufbewahrungsfristen der Daten. Eine Ausnahme von dem Grundsatz der Datensparsamkeit gilt freilich für journalistische Inhaltsdaten, die vom Medienprivileg erfasst sind. Die Zulässigkeit der Veröffentlichung personenbezogener Daten richtet sich hier nach den allgemeinen Regeln des Äußerungsrechts.

Regelmäßig sind sowohl die Inhaltsdaten als auch die Protokolldaten einer datenschutzrechtlichen Prüfung zu unterziehen. Zwischen den gesetzlichen Protokollierungspflichten als Vorkehrung zum Schutz der Daten einerseits und den datenschutzrechtlich geforderten Schutzvorkehrungen zum Schutz der informationellen

Selbstbestimmung der Arbeitnehmer/innen besteht ein erkennbarer Zielkonflikt. Die Protokollierung der Verarbeitungsvorgänge in einem Unternehmen ist notwendig, um die Verwendung der personenbezogenen Daten der Betroffenen nachvollziehen zu können. Andererseits bergen diese Daten ein Kontrollpotential zu Lasten der Beschäftigten, deren Tätigkeit am und um den Arbeitsplatz praktisch lückenlos nachvollzogen werden kann. Unter Abwägung dieser entgegenstehenden Interessen gilt es, jeweils eine sachgerechte Lösung zu finden.

## **1. RMS**

Am 1. 10. 2006 ist das neue Rechtemanagementsystem (RMS) in Betrieb gegangen. Das Modul RMS ist eine SAP-basierte Software, die die bisherigen Systeme zur Rechtedokumentation im Fernsehen ersetzt. Das System dient der Klärung von Rechte-Kosten für die Eigennutzung sowie Abgabe und Verwertung von Programmen, die im Wesentlichen in der Lizenzabteilung vorgenommen wird. Die Altsysteme FIDOS (SFB) und FRED (ORB) wurden nach der Übertragung der Datenbestände in RMS abgeschaltet.

Die vorausgegangene datenschutzrechtliche Prüfung hatte sich als schwierig erwiesen: Das Einführungsprojekt war bereits im Oktober 2005 gestartet. Es dauerte rund ein Jahr, um den Projektleiter davon zu überzeugen, dass für eine datenschutzrechtliche Prüfung des neuen Systems eine Reihe von Unterlagen wie der Katalog mit den Inhalts- und Nutzerdaten, das Berechtigungskonzept, die für die Nutzer- und Inhaltsdaten vorgesehenen Löschrufen und eine Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten vorgelegt werden müssen. Im Sommer 2006 habe ich schließlich einen Teil der Unterlagen erhalten, sodass ich dem Probetrieb ab Herbst 2006 zustimmen konnte. Es ist verabredet, dass mir die noch fehlenden Unterlagen für eine abschließende Prüfung nach und nach zur Verfügung gestellt werden.

## 2. Neues Dispositionssystem im rbb

Zurzeit wird noch mit unterschiedlichen Dispositionssystemen in den einzelnen Hörfunk-Programmen und im Fernsehen gearbeitet. Diese Anwendungen sind teilweise veraltet, fehlerhaft und basieren auf verschiedenen technischen Plattformen. Bereits im Frühjahr 2005 war ein Projektteam berufen worden, das zunächst den Auftrag hatte, ein einheitliches Dispositionssystem für den Hörfunk zu planen. Ich war von Anfang an in die Überlegungen mit einbezogen. Im Juni 2005 war das Anforderungsprofil für das neue Dispositions-System für den Hörfunk erstellt. Im Frühjahr 2006 wurde das Projekt unter neuer Projektleitung auf den Fernsehbereich erweitert. Im August/September 2006 wurden Teststellungen verschiedener Systeme vorgehalten. Während der Teststellungen wurden keine Echtdateien verwendet.

Anfang 2007 lag die Liste der Dispositionsdaten und das Leistungsverzeichnis vor. Bestandteil des Leistungsverzeichnisses ist unter anderem ein Berechtigungskonzept, das die verschiedenen Anwendergruppen (Rollen) und die Art der Autorisierung spezifiziert. Ferner wird im Leistungsverzeichnis ein Datensicherheitskonzept gefordert, das die Anforderungen der Dienstanweisung zur Verarbeitung personenbezogener Daten im **rbb** erfüllt. Inzwischen wurden einige Firmen aufgefordert, Angebote auf der Grundlage des Leistungsverzeichnisses abzugeben.

## 3. Ersatz des Online Content Management Systems (CMS)

Anfang 2007 hat die Abteilung Informations- und Kommunikationstechnik (IuK) gemeinsam mit der Online Koordination damit begonnen, die Migration der Online-Systeme auf eine neue Plattform vorzubereiten.

Die Technik weist keine großen Unterschiede zum bisherigen System auf. Es werden dieselben Rollen wie im alten System definiert. Es gibt eine Nutzerkennung für die Mitarbeiterinnen und Mitarbeiter und einen Passwortschutz. Die CMS-Logfiles werden für drei Monate vorgehalten und dann gelöscht. Eine Manipulation von außen ist ausgeschlossen, weil nicht direkt auf den Server des **rbb**, sondern auf eine

Spiegelung zugegriffen wird. Ich habe die Migration der Online-Systeme und die Änderung des Telemediengesetzes (s. B I 2. ) zum Anlass genommen, den gesamten Internetauftritt des **rbb** auf datenschutzrechtliche Zulässigkeit hin zu überprüfen. Die Prüfung dauert noch an.

#### 4. Bewerbermanagementsystem

Im August 2006 erhielt ich die Information aus der Abteilung Organisation und betriebswirtschaftliche IT-Systeme, dass der **rbb** die Einführung eines elektronischen Rekrutierungssystems für Auszubildende, Praktikanten und studentische Aushilfen plant. Durch die Einführung eines solchen Systems soll in erster Linie der Aufwand für die derzeit zeitintensive Bewerbungsprüfung und –verwaltung reduziert werden. Darüber hinaus sollen die Mitarbeiter/innen im Personalbereich bei der Korrespondenz mit den Bewerberinnen und Bewerbern sowie bei der Auskunftserstellung entlastet und die Portokosten reduziert werden. Zusammen mit dem IT-Sicherheitsbeauftragten habe ich die in das Leistungsverzeichnis aufzunehmenden datenschutz- und datensicherheitstechnischen Anforderungen definiert. Auch an dem Auswahlprozess der Anbieter war ich beteiligt. Mittlerweise hat sich der **rbb** für ein bestimmtes System entschieden. Das System wird voraussichtlich ab Sommer 2007 genutzt. Aus datenschutzrechtlicher Sicht ist folgendes hervorzuheben:

- ? Die Bewerbung in Papierform ist nach wie vor möglich.
- ? Das System ist AGG-konform.
- ? Die Datenfelder sind frei definierbar.
- ? Es gibt ein differenziertes Berechtigungskonzept.
- ? Die Archivierung der Dokumente ist revisionssicher.
- ? Die Übertragung der Daten erfolgt verschlüsselt.
- ? Auf dem Bewerbungsformular wird ein deutlicher Datenschutzhinweis erfolgen, der im Einzelnen mit mir abgestimmt wird.

## II. Organisatorische Regelungen

### 1. Dienstvereinbarung über die Einführung und Anwendung des Telekommunikationsanlagenverbundes

Am 28. 8. 2006 ist die neue Dienstvereinbarung über die Einführung und Anwendung des Telekommunikationsanlagenverbundes (DV TKAV) in Kraft getreten.

Zuvor waren die ehemaligen Dienstvereinbarungen des ORB und SFB zur Telefonnutzung sinngemäß weiter angewandt worden. Der Austausch der vorhandenen Einzeltelefonanlagen durch einen **rbb**-Telekommunikationsanlagenverbund Ende 2005 und die Notwendigkeit der Nutzung weiterer Funktionen waren Auslöser für die Aufnahme der Verhandlungen mit dem Personalrat über eine neue Dienstvereinbarung gewesen. An den Verhandlungen war ich beteiligt.

Vorrangiges Ziel der Dienstvereinbarung ist ausweislich Ziff. 1 Abs. 2 der Präambel der Schutz personenbezogener Daten und der Schutz des nicht öffentlich gesprochenen Wortes vor unberechtigten Eingriffen. In der Vereinbarung wird festgelegt, welche Funktionen und Leistungsmerkmale genutzt werden. Außerdem wird im Einzelnen aufgelistet, welche personenbezogenen Daten für welche Zwecke auf welche Weise verarbeitet werden. Bei abgehenden Telefongesprächen – dienstlichen und privaten – wird die um die letzten drei Ziffern gekürzte Zielrufnummer gespeichert und zu Abrechnungszwecken weiterverarbeitet. Bei ankommenden Telefongesprächen werden keine nebenstellenbezogenen Verbindungsdaten erfasst. Durch entsprechende technische und organisatorische Maßnahmen, die in der Dienstvereinbarung beschrieben sind, ist sichergestellt, dass die Vertraulichkeit auch sowohl bei der Abrechnung als auch beim Controlling gewahrt bleibt.

Ausdrücklich ist ein Abhörverbot in der Dienstvereinbarung geregelt. Aufzeichnungen von Telefongesprächen sind nur zulässig, wenn entweder das Einverständnis des Gesprächspartners mit der Aufzeichnung vorliegt, oder der Anruf eine strafbare Handlung (z. B. Drohanruf) darstellt. Die Telefone in der Telefonvermittlung sind auf besondere Weise gegen Drohanrufe geschützt. Sie sind an ein Dokumentationsystem angeschlossen. Am Telefon ist eine bestimmte Taste definiert, die im Falle

eines Drohanrufs zu betätigen ist. Wird nun ein Anruf über einen an dieses System angeschlossenen Apparat geführt, so wird während des Anrufes, prinzipiell von Anfang an, ein codiertes und nicht abhörbares Metafile im System erzeugt. Nach Beendigung des Telefongesprächs wird dieses Metafile wieder verworfen. Ein Abhören eines solchen Telefongesprächs ist nicht möglich, da keine verwertbaren Gesprächsdaten erzeugt werden. Sollte nun ein Drohanruf am Telefon erkannt werden, so betätigt die bedrohte Person die zur Drohanrufaufzeichnung eingerichtete Taste. Der Tastendruck wird vom System erkannt und aus dem Metafile wird ein Gesprächsfile, der dann in einem auswertbaren Format gespeichert wird. Es ist technisch sichergestellt, dass die Auswertung des aufgezeichneten Gesprächs ausschließlich von entsprechend autorisierten Personen in der Telefonvermittlung zusammen mit der Datenschutzbeauftragten bzw. dem IT-Sicherheitsbeauftragten vorgenommen wird.

## **2. Dienstvereinbarung über die Nutzung mobiler Telekommunikationsgeräte**

Ebenfalls am 28. 8. 2006 ist die Dienstvereinbarung über die Nutzung mobiler Telekommunikationsgeräte in Kraft getreten. Auch an den Verhandlungen über diese Dienstvereinbarung war ich intensiv beteiligt. Bis zu diesem Zeitpunkt waren die ehemaligen Dienstvereinbarungen von ORB und SFB sinngemäß angewandt worden.

Gegenstand der Dienstvereinbarung ist die Nutzung und Abrechnung mobiler Telekommunikationsgeräte, die den Mitarbeiterinnen und Mitarbeitern für dienstliche Zwecke zur Verfügung gestellt werden. Dienstliche mobile Telekommunikationsgeräte dürfen nur dann privat genutzt werden, wenn diese neben dem dienstlichen Anschluss einen zweiten privaten Anschluss mit separater Rufnummer besitzen. Die Kosten des privaten Anschlusses werden den Nutzern des Geräts direkt durch den Mobilfunkanbieter in Rechnung gestellt. In der Dienstvereinbarung ist festgelegt, dass der **rbb** mit den Mobilfunkanbietern vereinbart, die Zielrufnummern von dienstlichen Anschlüssen um die letzten drei Ziffern gekürzt zu speichern.

Durch entsprechende technische und organisatorische Maßnahmen, die in der Dienstvereinbarung im Einzelnen geregelt sind, ist sichergestellt, dass die Vertraulichkeit der Daten auch bei der Abrechnung und beim Controlling gewahrt wird.

### **3. Richtlinien für den Einsatz von Externen bei der Wartung von IT- und TK-Systemen**

Im Oktober 2006 sind die Richtlinien für den Einsatz von Externen bei der Wartung von IT- und TK-Systemen vom Verwaltungsdirektor und Betriebs- und Produktionsdirektor gemeinsam für ihre jeweiligen Direktionen erlassen worden. Den Entwurf der Richtlinien hatte ich zusammen mit einigen Kollegen aus den beiden Direktionen und dem IT-Sicherheitsbeauftragten erarbeitet.

Der Einsatz von externen Firmen bei der Wartung von IT- und TK-Systemen ist inzwischen üblich. Er birgt allerdings Gefahren für den Schutz personenbezogener Daten und für die Datensicherheit in sich. Das gilt insbesondere dann, wenn dem Fremdpersonal Zugang zum Hausnetz gewährt werden muss.

In § 3 a BerlDSG, der über § 36 **rbb**-Staatsvertrag Anwendung findet, sind für die sog. Fremdwartung spezielle Anforderungen geregelt.

Die darin enthaltenen abstrakten Regelungen dienen insbesondere dazu, eine umfassende Kontrolle der Wartungsarbeiten durch den Auftraggeber sicherzustellen. Außerdem soll ausgeschlossen werden, dass bei der Wartung Programme und Daten aufgerufen werden können, die für die Arbeit der Fremdfirmen nicht benötigt werden.

In den „Richtlinien für den Einsatz von Externen bei der Wartung von IT- und TK-Systemen“ werden die in § 3 a BerlDSG abstrakt formulierten Pflichten konkret umgesetzt. Es wird u. a. detailliert festgelegt, welche Regelungen zur Sicherstellung von Datenschutz und Datensicherheit mit den externen Firmen vertraglich vereinbart werden müssen. Außerdem werden die von den **rbb**-Mitarbeiterinnen- und –Mitarbeitern vor, während und nach dem Einsatz von Fremdpersonal zu treffenden Maßnahmen festgelegt. Ein Schwerpunkt ist dabei die Durchführung des Fern-

zugriff-Verfahrens, bei dem von außen via Internet auf das **rbb**-Netz zugegriffen wird.

Der Inhalt der Richtlinien wird seit Oktober 2006 bei Änderungen oder Neuabschlüssen von Wartungsverträgen regelmäßig Vertragsbestandteil.

### III. Sonstiges

#### 1. Stasi-Überprüfung im rbb

Auf Empfehlung des Rundfunkrates vom 8. 9. 2003 fand im **rbb** eine Überprüfung der Programm prägenden und leitenden fest angestellten sowie der Programm prägenden freien Mitarbeiter/innen des **rbb** auf eine etwaige Zusammenarbeit mit dem Ministerium für Staatssicherheit der DDR statt.

Für die fest angestellten Mitarbeiter/innen wurde vom **rbb** ein entsprechender Auskunftsanspruch gestellt. Die freien Mitarbeiterinnen und Mitarbeiter wurden gebeten, selbst die entsprechenden Auskünfte der BIRTHLER-Behörde über sich einzuholen und dem **rbb** das Original oder eine Kopie der Auskunft zur Verfügung zu stellen.

Nach Abschluss der Überprüfung im Sommer 2006 erhielten sämtliche fest angestellten Mitarbeiter eine Nachricht vom **rbb** über die von der BIRTHLER-Behörde erteilten Auskünfte. Die Original-Schreiben der BIRTHLER-Behörde werden seit dem Frühjahr 2007 in den Magazinen des Landeskirchlichen Archivs im Kirchlichen Archivzentrum Berlin gesondert und unter Verschluss für den **rbb** aufbewahrt. Den zugrunde liegenden Archivierungsvertrag hatte ich als Datenschutzbeauftragte geprüft. Jede/r Betroffene hat selbstverständlich ein Recht auf Einsicht in das sie/ihn betreffende Schreiben.

Ich habe empfohlen, die Schreiben längstens für die Dauer der Tätigkeit des jeweiligen Mitarbeiters aufzubewahren, verbunden mit der Zusage, diese mit Ausscheiden aus dem Beschäftigungsverhältnis zu vernichten bzw. an die BIRTHLER-Behörde zurückzusenden. Nach fünf Jahren soll unter Berücksichtigung der aktuellen Gesetzesentwicklungen und der arbeitsgerichtlichen Rechtsprechung allgemein überprüft

werden, ob das Dokumentationsinteresse für die Unterlagen überhaupt noch weiter besteht.

## 2. Diverse Einzelvorgänge

Im Berichtszeitraum gab es diverse Einzelanfragen aus unterschiedlichen Bereichen, die ich entweder telefonisch oder schriftlich beantwortet habe.

Vom Personalrat wurde beispielsweise die Frage an mich herangetragen, ob der Fachvorgesetzte die Herausgabe der privaten Telefonnummer verlangen kann. Ich habe dazu wie folgt Stellung genommen: In den Fällen, in denen der/die entsprechende Mitarbeiter/in über ein bestimmtes Spezialwissen verfügt, ist es zulässig, ihn während einer unvorhergesehenen Abwesenheit (z. B. wegen Krankheit) im Notfall zu Hause anzurufen. Für einen derartigen Fall kann der/die Vorgesetzte vorsorglich die Bekanntgabe der privaten Telefonnummer verlangen.

Eine Studentin hat sich an die Personalabteilung gewandt und für eine Diplomarbeit die Herausgabe einer Liste mit den im **rbb** beschäftigten schwer behinderten Journalistinnen und Journalisten gebeten. Ich habe der Personalabteilung empfohlen, diese Bitte abschlägig zu bescheiden. Das ist inzwischen geschehen.

Durch Zufall erfuhr ich, dass Mitarbeiterinnen und Mitarbeiter von externen Firmen, die beispielsweise für die Prüfung der Elektroanschlüsse in den Büros zuständig sind, nicht durchgängig eine Vertraulichkeitserklärung gegenüber dem **rbb** abgegeben haben. Ich habe die zuständige Abteilungsleiterin gebeten, die Einholung derartiger Erklärungen umgehend nachzuholen und sie zukünftig – wie bei den Wartungsverträgen im IT-Bereich - zum Inhalt des Vertrages mit den Wartungsfirmen zu machen.

Das im **rbb** eingesetzte Reinigungsunternehmen hat dem **rbb** im Februar 2007 in einer Präsentation eine neue mögliche digitale Steuerung des Reinigungsablaufs vorgestellt. Hierbei soll jede Mitarbeiterin und jeder Mitarbeiter der Reinigungsfirma mit einem Handheld-Gerät (Pocket-PC) ausgestattet und jeder Raum im **rbb**-

Gebäude mit einem Chip versehen werden. Somit würde nicht nur die Dauer der Reinigung nachvollziehbar, sondern auch die Reinigungsleistung für jeden Raum individuell steuerbar. Der **rbb** könnte über das Internet im Portal der Firma seine Aufträge, Sonderwünsche, Beschwerden etc. direkt platzieren. Eine Übertragung der Daten erfolgte dann per GPS an das entsprechende Handheld-Gerät der Firma. Die Firma beabsichtigt am Standort Berlin in einem Bereich, welcher noch zu bestimmen ist, ein Pilotprojekt durchzuführen. Ich wurde um eine Überprüfung gebeten, ob aus datenschutzrechtlichen Gründen Einwände bestehen.

Ich habe der zuständigen Abteilungsleiterin mitgeteilt, dass ich gemäß BerlDSG nur für den Schutz der personenbezogenen Daten der **rbb**-Mitarbeiterinnen und –Mitarbeiter zuständig bin. Im Wesentlichen wären ja die Mitarbeiterinnen und Mitarbeiter der Reinigungsfirma von der Maßnahme betroffen. Deshalb habe ich gegen das Projekt keine grundsätzlichen Einwände erhoben.

Ich habe aber darum gebeten, mich in die konkreten Vorbereitungsarbeiten mit einzubeziehen, sollte es tatsächlich zu der Durchführung des Pilotprojekts kommen, weil voraussichtlich auch einige personenbezogenen Daten der **rbb**-Mitarbeiterinnen und Mitarbeiter als Empfänger/innen der Reinigungsleistungen, bei den entsprechenden Meldungen anfallen werden.

#### **IV. Schulungen**

Am 14. August 2006 führte ich zusammen mit dem Systemverantwortlichen für IT-Sicherheit, Herrn Gerry Wolff, ein Einführungsseminar zum Thema „Datenschutz und Datensicherheit im **rbb**“ für unsere neuen Auszubildenden durch. An unseren Vortrag schloss sich eine angeregte Diskussion an, in der viele praktische Themen vertieft werden konnten.

## D. Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung

### I. Allgemeines

Für die Einziehung der Rundfunkgebühren ist seit 1976 die Gebühreneinzugszentrale (GEZ) in Köln zuständig. Die GEZ ist eine öffentlich-rechtliche nicht rechtsfähige Verwaltungsgemeinschaft der Landesrundfunkanstalten, des ZDF und des Deutschlandradio. Rechtsgrundlage ist eine zwischen den Rundfunkanstalten abgeschlossene Verwaltungsvereinbarung.

Der bei der GEZ geführte Rundfunkteilnehmer-Datenbestand umfasste per Ende Dezember 2006 rund 39,5 Mio. Teilnehmerkonten mit insgesamt angemeldeten rund 42,8 Mio. Hörfunkgeräten und 36,9 Mio. Fernsehgeräten (davon gebührenpflichtig 39,3 Mio. Hörfunk- und 33,7 Mio. Fernsehgeräte, gebührenbefreit 3,5 Mio. Hörfunk- und 3,2 Mio. Fernsehgeräte). Für den **rbb** waren Ende 2006 rund 2,9 Mio. Hörfunkgeräte angemeldet, davon waren 0,3 Mio. Geräte (= 12,08 %) befreit. Von den rund 2,6 Mio. Fernsehgeräten waren ebenfalls 0,3 Mio. Geräte (= 13,29 %) befreit.

Für die routinemäßige Sachbearbeitung ist nach den Festlegungen in der Verwaltungsvereinbarung und ergänzenden organisatorischen Regelungen die GEZ zuständig. Das gilt auch für die Durchführung der Befreiungen von natürlichen Personen. Bei den Landesrundfunkanstalten verbleiben die folgenden Aufgaben, soweit keine andere Vereinbarung im Einzelfall getroffen wurde:

- Beauftragtendienst (Organisation, Steuerung, Überwachung etc.),
- Bearbeitung besonders gekennzeichnete Teilnehmerkonten, für die die Landesrundfunkanstalt aus besonderen Gründen die Betreuung übernommen hat,
- Regelungen für Stundung, Niederschlagung und Erlass von Rundfunkgebühren,
- Abwicklung des Befreiungsverfahrens einschl. Bestandsveränderungen für besondere Betriebe und Einrichtungen mit Ausnahme der Bestandsführung,
- Abwicklung von Widersprüchen gegen Gebührenbescheide sowie gegen Befreiungsbescheide,

- Einleitung von Verwaltungszwangsverfahren wegen Auskunftsverweigerung,
- Einleitung von Ordnungswidrigkeitenverfahren wegen Nichtanmeldung,
- Klärung aller rechtlichen Grundsatzfragen und
- Führen von Rechtsstreitigkeiten in Rundfunkgebührenangelegenheiten

Die personenbezogenen Teilnehmerdaten werden ausschließlich zum Zweck des Gebühreneinzugs erhoben und weiterverarbeitet. Für die Datenschutzkontrolle ist jeweils der/die Rundfunkdatenschutzbeauftragte der einzelnen Rundfunkanstalt für den entsprechenden Teilnehmerkreis zuständig. Unterstützt werden die Rundfunkdatenschutzbeauftragten durch die interne Datenschutzbeauftragte der GEZ, Frau Kerstin Arens. In den Ländern Berlin, Brandenburg, Bremen und Hessen ist durch entsprechende gesetzliche Regelungen den staatlichen Datenschutzbeauftragten diese Kontrollfunktion zugewiesen.

Für den Datenschutz der Rundfunkteilnehmer/innen gelten in erster Linie die bereichsspezifischen Regelungen des Rundfunkgebührenstaatsvertrags und – für die Teilnehmer in Berlin und Brandenburg - gemäß § 36 Abs. 1 **rbb**-Staatsvertrag ergänzend das Berliner Datenschutzgesetz. Das gilt auch für die Verarbeitung der Daten durch die GEZ, die insoweit Auftragsdatenverarbeiter des **rbb** ist (§ 8 Abs. 2 Rundfunkgebührenstaatsvertrag).

Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung und Beantwortung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten der Datenschutzbeauftragten der GEZ übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben sie sich selbst vorbehalten.

Im Jahr 2006 hat die Datenschutzbeauftragte der GEZ folgende Vorgänge aus dem Sendegebiet des **rbb** für mich bearbeitet:

Ersuchen von Rundfunkteilnehmern um Auskunft über zu ihrer Person gespeicherte Daten	9
Fragen bezüglich der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung	16
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen	22
Verlangen, Teilnehmerdaten nicht zu anderen Zwecken zu nutzen bzw. zu übermitteln	0
Anfragen von Finanzämtern nach Daten (insbes. Bankverbindungen) von Rundfunkteilnehmern	22
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Rundfunkteilnehmern	1
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz	3
<b>Anzahl Vorgänge insgesamt:</b>	<b>73</b>

Ich selbst habe folgende Vorgänge bearbeitet:

Bitte um Kontenklärung mit entsprechender Aufstellung der Zahlungseingänge	1
Fragen bezüglich der Herkunft der Daten (z. B. Adressen) bzw. der Berechtigung zur Datenerhebung	2
Fragen im Zusammenhang mit der Glaubhaftmachung der Befreiungsvoraussetzungen	3
Beschwerde über das Vorgehen eines Rundfunkgebühren-Beauftragten	3
Auskunftersuchen über die zur eigenen Person gespeicherten Daten	4
<b>Anzahl Vorgänge insgesamt:</b>	<b>13</b>

Die Anfragen der Finanzämter und Kommunalkassen werden aus datenschutzrechtlichen Gründen grundsätzlich abschlägig beschieden.

Zu allen Eingaben konnte der Sachverhalt aufgeklärt und den Betroffenen eine zufrieden stellende Antwort gegeben werden. Verstöße gegen datenschutzrechtliche Vorschriften wurden dabei nicht festgestellt.

Die Anzahl der Anfragen oder Beschwerden zu Fragen des Datenschutzes beim Einzug der Rundfunkgebühren und speziell auch zu Mailingmaßnahmen ist – gemessen an der Menge der Rundfunkteilnehmer, dem Gesamtvolumen des Mailings bzw. der insgesamt angefallenen Geschäftsvorgänge – nach wie vor als gering und unkritisch zu sehen.

## **II. GEZ**

### **1. Konsolidierungsarbeiten zum Projekt DV2005**

In meinen früheren Tätigkeitsberichten habe ich ausführlich über die Umstellung auf das neue Datenverarbeitungssystem bei der GEZ „DV 2005“ zum 11. 7. 2005 berichtet. Erwartungsgemäß waren auch im Berichtszeitraum noch weitere begleitende Prüfungen und Beratungen erforderlich. Inzwischen sind einige Mängel, die das System noch aufwies, behoben worden.

### **2. Neues Löschkonzept**

Im Sommer 2006 wurde das Löschkonzept zu Daten der Teilnehmerhistorie aus dem Jahr 1995 aktualisiert. Auslöser war die Inbetriebnahme des neuen DV-Systems „DV 2005“ ab dem 11.7. 2005. Das neue System kennt keine Funktionscodes mehr, sondern arbeitet mit dem Begriff der Geschäftsvorfälle, von denen weit mehr existieren, als Funktionscodes im Altsystem vorhanden waren. Hinzu kam die Tatsache, dass sich auch die maßgeblichen gesetzlichen Fristen für den Gebühreneinzug (u. a. im RGebStV) inzwischen geändert hatten.

An der Überarbeitung des neuen Löschkonzepts habe ich maßgeblich mitgewirkt. Gegenüber dem bisherigen Historielöschkonzept, in dem eine Vielzahl von Funktionscodes als so genannte „Fundamentaldaten“ unbefristet gespeichert wurden, wurde die Gruppe derartiger Fundamentaldaten in Abstimmung mit allen betroffenen Bereichen erheblich verringert. Alle übrigen Geschäftsvorfälle bzw. die entsprechenden Funktionscodes aus dem Altsystem wurden als „Nicht-Fundamentaldaten“ definiert, die grundsätzlich einer Speicherdauer von 3 Jahren zuzüglich des laufenden Jahres unterliegen. Zum Teil ist dies an Bedingungen geknüpft, die aus dem bisherigen Konzept übernommen wurden. Zum Teil kommen auch längere Fristen (10 Jahre/30 Jahre) zum Tragen. Alle vorgesehenen Fristen korrespondieren mit entsprechenden gesetzlichen Regelungen.

### **3. Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Bremen, Hessen, Berlin und Brandenburg**

Wie bereits in meinen früheren Tätigkeitsberichten berichtet, haben die Landesdatenschutzbeauftragten von Hessen, Bremen, Berlin und Brandenburg in der Zeit vom 21. bis 23. 9. 2004 die GEZ geprüft. In ihrem Prüfbericht aus dem Juni 2005 hatten die Landesdatenschutzbeauftragten u. a. § 8 Abs. 4 RGebStV die Geeignetheit als Rechtsgrundlage für die Mailing-Aktionen der GEZ abgesprochen, einzelne Passagen der Informationsschreiben der GEZ an potentielle Rundfunkteilnehmer kritisiert und die Notwendigkeit der Zugriffsmöglichkeit für jede Sachbearbeiterin und jeden Sachbearbeiter bei der GEZ auf sämtliche Teilnehmerkonten in Deutschland bestritten sowie einzelne Details des Löschkonzepts kritisiert. Mit Schreiben vom 17. Februar 2006 hat die Intendantin die gemeinsame Stellungnahme der von der Prüfung unmittelbar betroffenen Rundfunkanstalten dem Berliner Beauftragten für Datenschutz und Informationsfreiheit übermittelt. An der Stellungnahme hatte ich intensiv mitgewirkt. Die Rundfunkanstalten haben in ihrer Stellungnahme dargelegt, dass und warum sie § 8 Abs. 4 RGebStV für eine geeignete Rechtsgrundlage für die Anmietung von Adressen bei privaten Adresshändlern zur Durchführung von Mailing-Maßnahmen halten. Die Musterbriefe, die bei den Mailing-Maßnahmen verwendet werden, und deren Wortlaut nicht - wie in der Vergangenheit üblich - zuvor mit den Mitgliedern des AK DSB abgestimmt worden waren, wurden inzwischen überarbeitet. Daran war ich maßgeblich beteiligt. An der Notwendigkeit der

Möglichkeit des bundesweiten Zugriffs der Sachbearbeiterinnen und Sachbearbeiter bei der GEZ und in der Rundfunkgebührenstelle halten die Rundfunkanstalten fest. Das Löschkonzept ist im Zuge der Umstellung auf das neue DV System und vor dem Hintergrund der geänderten Verjährungsvorschriften unter meiner Mitarbeit überarbeitet worden (s. 2.)

Zu dem Schreiben der Intendantin und der Intendanten haben sich mit Schreiben vom 25. Januar 2007 noch einmal die Landesdatenschutzbeauftragten zu Wort gemeldet. Sie halten u. a. weiterhin an der Kritik zu einzelnen Formulierungen in den Mailing-Briefen fest und stellen erneut die Erforderlichkeit der Möglichkeit des bundesweiten Zugriffs der Rundfunkgebührenbeauftragten auf die Rundfunkteilnehmerkonten in Frage. Eine Antwort der Intendantin und der Intendanten auf das jüngste Schreiben der Landesdatenschutzbeauftragten steht noch aus. Zwischenzeitlich stattgefundenen Gespräche mit den beim Berliner und Brandenburgischen Landesdatenschutzbeauftragten für Medien zuständigen Sachbearbeitern haben gezeigt, dass es nach wie vor einige Missverständnisse zum Thema „Zugriffsmöglichkeiten auf die Datenbank der GEZ“ gibt. Möglicherweise werden die Landesdatenschutzbeauftragten ihre Kritik an dem Verfahren nach ergänzenden Erläuterungen nicht länger aufrecht halten.

#### **4. Verfahren bei der Befreiung von der Rundfunkgebühr**

Seit dem 1. 4. 2005 obliegt der GEZ das Verfahren zur Befreiung natürlicher Personen von der Rundfunkgebührenpflicht, welches zuvor von den Sozialbehörden wahrgenommen wurde. Die Rundfunkgebührenbefreiung wird nur auf Antrag und bei Vorliegen bestimmter sozialer Leistungen bzw. eines RF-Merkzeichens gewährt. Der Antragsteller hat gemäß § 6 Abs. 2 RGebStV das Vorliegen der Befreiungsvoraussetzungen durch die Vorlage bestimmter Leistungsbescheide im Original oder in beglaubigter Kopie nachzuweisen. Da auf den der GEZ vorzulegenden Bescheiden auch viele sensible Daten enthalten sind, die für die Befreiungsbearbeitung nicht benötigt werden, ist von vielen Seiten - u. a. von den Landesdatenschutzbeauftragten von Berlin und Brandenburg und dem Verwaltungsgericht Berlin – Kritik an der derzeitige gesetzlichen Regelung geäußert worden. Zum Teil werden sogar verfas-

sungsrechtliche Bedenken geäußert. Die Rundfunkdatenschutzbeauftragten teilen diese Kritik.

Aus diesem Grund hat die GEZ eine Lösung für eine verfassungskonforme Anwendung der gesetzlichen Regelungen entwickelt: Sie akzeptiert sog. Drittbescheide von den Sozialleistungsträgern, auf denen nur die für die Befreiung relevanten Daten aufgeführt sind. Für die Sozialbehörden besteht dadurch kein nennenswerter zusätzlicher Aufwand, weil das Ausstellen der Drittbescheinigungen in die entsprechenden Fachverfahren implementiert werden kann. Außerdem entfällt der Aufwand für das Kopieren und Beglaubigen. Eine Verpflichtung, Drittbescheinigungen auszustellen, wird aber von den kommunalen Spitzenverbänden und den Spitzenverbänden der Sozialleistungsträger abgelehnt, weil dort ein zusätzlicher finanzieller Aufwand befürchtet wird. Deshalb favorisieren die Staatskanzleien eine freiwillige Lösung und wollen durch eine entsprechende Änderung von § 6 Abs. 2 RGebStV im 10. Rundfunkänderungsstaatsvertrag lediglich die Möglichkeit vorsehen, eine Drittbescheinigung auszustellen. Konkrete Formulierungsvorschläge wurden mit den Rundfunkanstalten, den Rundfunkdatenschutzbeauftragten und den Landesdatenschutzbeauftragten abgestimmt (s. B I 3).

Nach wie vor strebt die GEZ ein flächendeckendes Verfahren zur elektronischen Übermittlung der für die Befreiung erforderlichen Leistungsbescheidsdaten an. Das Verfahren zur elektronischen Datenübermittlung zwischen der GEZ und den Landesversorgungsämtern befindet sich seit dem 1. 1. 2007 im produktiven Einsatz. Pilotanwender ist das Landesversorgungsamt Münster, das für das Bundesland Nordrhein-Westfalen zuständig ist. Aufgrund der ersten Anträge von Teilnehmern, die dem elektronischen Datenaustausch mit einer unterschriebenen Einverständniserklärung zugestimmt haben, findet seit Anfang Februar 2007 der elektronische Datenaustausch statt. Nach dem erfolgreichen Abschluss der Pilotphase wird parallel zur Einführung bei den übrigen Landesversorgungsämtern die Möglichkeit der elektronischen Datenübermittlung mit den Kommunen angestrebt. Auch mit der Bundesanstalt für Arbeit wird weiter verhandelt. Leider gibt es dort nach wie vor erheblichen Widerstand. Bei den Bemühungen um Akzeptanz bei den Behörden

werden die GEZ und die Landesrundfunkanstalten auch intensiv durch die staatlichen Datenschutzbeauftragten unterstützt.

## **5. NP-Datenbank**

Wie bereits in meinem vorhergehenden Tätigkeitsbericht ausgeführt, finden bei der GEZ intensive Vorbereitungen für die Einrichtung einer sog. NP-Datenbank statt, um eine zielgerichtete Bearbeitung und Ausschöpfung des NP(=Nichtprivaten)-Marktes zu gewährleisten. In der NP-Datenbank werden voraussichtlich auch personenbezogene Daten, z. B. von Einzelkaufleuten und Freiberuflern, gespeichert. Der Arbeitskreis der Datenschutzbeauftragten von ARD und ZDF hatte –wie berichtet – die im Rahmen einer Sitzung am 7.11.2005 präsentierte Version einer NP-Datenbank für nicht vertretbar gehalten, insbesondere aufgrund der dauerhaften Speicherung der Daten und deren Umfang. Daraufhin fanden im Frühjahr 2006 unter der Moderation des Justitiars des Hessischen Rundfunks und Mitglieds des Verwaltungsrats der GEZ, Herrn Conrad Schraube, Gespräche zwischen den Leitern der Abteilung Rundfunkgebühren und den Mitgliedern des AK DSB zur Lösung der datenschutzrechtlichen Probleme statt. Dabei verständigte man sich auf eine höchstzulässige Speicherdauer von 12 Monaten. Außerdem wurde u. a. eine Speicherung von Namen der Geschäftsführer/Vorstandsmitglieder ebenso für zweckdienlich und zulässig erachtet wie eine Speicherung von im Geschäftsverkehr genutzten Kommunikationsdaten von Ein-Personen-Gesellschaftern/Freiberuflern. Geplant ist, dass sowohl die GEZ als auch die Landesrundfunkanstalten und der Beauftragten dienst einen bundesweiten Zugriff auf die NP-Datenbank erhalten. Das Fachkonzept zur NP-Datenbank ist inzwischen unter Berücksichtigung der definierten Eckpunkte überarbeitet. Der AK DSB hat sich in seiner Sitzung am 21./22. September 2006 in Bremen mit dem überarbeiteten Konzept befasst und festgestellt, dass keine grundlegenden Bedenken mehr bestehen und dass das Konzept im Grundsatz als akzeptabel angesehen wird. Allerdings wird der Online-Zugriff der Gebührenbeauftragten für problematisch eingestuft. Hierzu gibt es offenbar bislang keine näheren konzeptionellen Festlegungen. Seitdem ist der AK DSB noch nicht wieder mit dem Thema befasst worden.

### **III. Rundfunkgebührenabteilung**

Mit dem Leiter der Abteilung Rundfunkgebühren, Herrn Gerald Schermuck, befinde ich mich in einem permanenten regen Austausch über datenschutzrechtliche Fragen im Zusammenhang mit der Sachbearbeitung in der Abteilung, aber auch mit der Datenverarbeitung durch die Rundfunkgebührenbeauftragten, die als freie Mitarbeiterinnen und Mitarbeiter für den **rbb** vor Ort die Einhaltung der Gebührenpflicht überprüfen. Zum 1. 1. 2007 wurden die Verträge mit den Rundfunkgebührenbeauftragten hinsichtlich der Vergütungsmodalitäten geändert. Ich habe dies zum Anlass genommen, auch die datenschutzrechtlichen Festlegungen in den Verträgen zu aktualisieren.

Regelmäßig führe ich gemeinsam mit dem IT-Sicherheitsbeauftragten Schulungen zum Thema Datenschutz mit den Rundfunkgebührenbeauftragten durch. Die Landesdatenschutzbeauftragten von Berlin und Brandenburg haben für den Sommer 2007 eine ausführliche datenschutzrechtliche Prüfung einzelner Rundfunkgebührenbeauftragter angekündigt.

## **E. Datenschutz im Informationsverarbeitungszentrum (IVZ)**

### **I. Allgemeines**

Das Informationsverarbeitungszentrum ist ein gemeinsames Rechenzentrum von MDR, **rbb**, Radio Bremen, NDR, SR und DLR (die vier letztgenannten sind Teilkooperationspartner) mit Sitz in Potsdam. Für die datenschutzrechtliche Kontrolle sind alle Datenschutzbeauftragten der Betreiber-Anstalten gemeinsam zuständig. Federführend wird die Arbeit von mir als der Datenschutzbeauftragten vor Ort durchgeführt.

## **II. Einzelne Themen**

### **1. BSI-Zertifizierung**

Das IVZ strebt eine Zertifizierung hinsichtlich der Einhaltung der datenschutz- und datensicherheitstechnischen Bestimmungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) an. Die Zertifizierung wird jeweils für zwei Jahre befristet ausgesprochen.

Die Datenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten sind an den Vorbereitungsarbeiten dafür seit Frühjahr 2006 beteiligt. In einem ersten Schritt wurde der Schutzbedarf für die Daten definiert. Inzwischen sind eine Reihe von Dokumenten, Arbeitsanweisungen u.ä. erstellt und technische Sicherheitsvorkehrungen umgesetzt worden. Das IVZ hofft, die Zertifizierung im Sommer 2007 zu erlangen.

### **2. Dokumentenmanagement im IVZ**

Das IVZ hat im Frühjahr 2007 Teile eines Dokumentenmanagement-Systems (DMS) eingeführt, um folgende im IVZ anfallenden Dokumente elektronisch zu verwalten:

- ? Selbst erstellte System- und Anwenderdokumentationen,
- ? Von Zulieferern übergebene Dokumentationen,
- ? Grafiken und Tabellen, die die Inhalte der IT-Systeme des IVZ beschreiben,
- ? Projektprotokolle,
- ? Protokolle der IVZ-Ressortleiterbesprechungen und
- ? Unterlagen für Verwaltungsrat- und Lenkungsausschusssitzungen (Gremien-dokumente).

Die meisten Dokumente werden von IVZ- Mitarbeitern erstellt und gepflegt. In Papierform übergebene Dokumente von Zulieferern bzw. Mitarbeitern aus den Rundfunkanstalten werden gescannt und sofort in das DMS übernommen. Diese Dokumente werden auch weiterhin in Papierform aufbewahrt. Der Kreis der Zugriffsberechtigten setzt sich derzeit aus folgenden Personen zusammen: Mitarbeiterinnen

und Mitarbeiter des IVZ – auch an den Außenstandorten -, Mitglieder des IVZ-Verwaltungsrats und Mitglieder des IVZ-Lenkungsausschusses.

Bei der von mir zusammen mit dem IT-Sicherheitsbeauftragten durchgeführten Vorabkontrolle habe ich mich davon überzeugen können, dass es einen angemessenen Zugangsschutz (über Benutzername und Passwort) und ein differenziertes Berechtigungskonzept gibt. Lesende Zugriffe werden nicht protokolliert, für schreibende Zugriffe werden der Änderungszeitpunkt und der Name des Ändernden gespeichert. Für jeden Benutzer einsehbar sind die Daten der letzten Änderung, für ältere Versionen wird nur der Änderungszeitpunkt angezeigt. Das Einscannen von Dokumenten erfolgt nicht automatisiert. Der Datenschutz wird bei diesem Vorgang durch entsprechende organisatorische Maßnahmen gewährleistet.

In dem System sind Funktionalitäten wie Archivierung nach Fristen, automatisiertes Löschen von Daten etc., wie sie einem klassischen Dokumentenmanagementsystem immanent sind, nicht vorgesehen. Die Dokumentenpflege obliegt daher dem jeweiligen Dokumenteneigner. Ich habe den Geschäftsführer des IVZ gebeten, Herrn Dr. Georg Greten, durch entsprechende Anweisungen gegenüber seinen Mitarbeitern sicherzustellen, dass die personenbezogenen Daten gelöscht werden, sobald ihre Aufbewahrung nicht mehr erforderlich ist.

### **3. Telearbeitsplätze**

Anfang 2006 wurde beim IVZ ein auf zwei Jahre befristeter Pilotversuch zur partiellen Telearbeit für SAP-Entwickler gestartet. Die datenschutzrechtlichen Anforderungen für den häuslichen Arbeitsplatz und die technische Verbindung zwischen IVZ und Heimarbeitsplatz wurden von den Datenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten vorgegeben. Die entsprechenden Verpflichtungen wurden in eine Zusatzvereinbarung zum Arbeitsvertrag festgelegt.

Technisch sichergestellt ist, dass die Mitarbeiter nicht auf die Produktivsysteme zugreifen können. Die Datenschutzbeauftragten haben die Anbindung über VPN RemoteAccess zwar grundsätzlich als sicher eingestuft, jedoch empfohlen den

Zugriff auf die Entwicklungs- und Testumgebung zu beschränken, da der Zugriff auf die Produktivsysteme ohnehin nur in seltenen Ausnahmefällen erforderlich ist.

Seit Beginn des Pilotversuchs hat es keine Datenschutz- und Datensicherheitsprobleme gegeben. Im September 2007 wird der Verwaltungsrat des IVZ über die Weiterführung des Pilotprojekts entscheiden.

## I. Organisatorische Regelungen

Mit Schreiben vom 13. 12. 2006 hat Herr Dr. Greten mich darüber informiert, dass er Anfang 2006 die **rbb**-Dienstanweisung zur Nutzung von Internet und E-Mail, die an die Situation im IVZ (Outlook) angepasste Lotus-Notes-Dienstanweisung und die **rbb**-Datenschutz-Dienstanweisung an alle Mitarbeiterinnen und Mitarbeiter des IVZ verteilt habe.

Die in den Regelungen vorgesehenen Vertraulichkeitserklärungen seien von allen Mitarbeiterinnen und Mitarbeitern unterschrieben worden.

## F. Datenschutz im ARD-Hauptstadtstudio (HSB)

Anfang März 2007 hat die Verwaltungsleitung des ARD-Hauptstadtstudios (HSB) dem **rbb**-Justitiariat eine an die technischen und organisatorischen Gegebenheiten beim HSB angepasste Version der **rbb**-Dienstanweisungen zur Verarbeitung personenbezogener Daten, für die Nutzung von Internet und e-Mail und für die Nutzung von Lotus Notes zur Prüfung zugeleitet. In meiner Eigenschaft als Datenschutzbeauftragte wurde ich in die Prüfung mit einbezogen. Im Sommer 2007 sollen die modifizierten Dienstanweisungen in Kraft treten.

Im Rahmen der Einführung von Zertifikaten (vertrauenswürdigen digitalen Signaturen) für Server arbeitet der **rbb** mit dem HSB zusammen. Es wurde ein gemeinsames System für die Beantragung und Ausstellung von Zertifikaten beim DFN-Verein installiert. Somit erkennt man sichere und vertrauenswürdige Systeme von rbb und HSB im Internet, wenn man auf diese via Fernzugänge zugreift.

Für die Zukunft beabsichtige ich, den Erfahrungsaustausch mit dem Verantwortlichen für die IT-Systeme im HSB wieder zu intensivieren.

## **G. Sonstiges**

### **I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR**

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten arbeiten im Arbeitskreis der Datenschutzbeauftragten (AK DSB) zusammen. Der Vorsitz des AK DSB wechselt regelmäßig alle zwei Jahre. Gegenwärtig hat der Datenschutzbeauftragte des WDR, Herr Thomas Drescher, den Vorsitz inne. Ich bin seit einigen Jahren stellvertretende Vorsitzende des Arbeitskreises.

Auf unseren Sitzungen informieren wir uns gegenseitig über Entwicklungen auf dem Gebiet der Datenschutzgesetzgebung und erarbeiten gemeinsame Stellungnahmen. Ferner findet ein Erfahrungsaustausch in der praktischen Durchführung des Datenschutzes im Betrieb statt. Ein wichtiges Ziel ist überdies, den Datenschutz beim Rundfunkgebühreneinzug nach möglichst einheitlichen Kriterien – d. h. in der Praxis nach den jeweils höchsten Anforderungen – sicherzustellen. Die Datenschutzbeauftragte der GEZ ist Mitglied des Arbeitskreises.

Im Berichtszeitraum fand eine reguläre Sitzung des AK DSB am 21./22. September 2006 bei Radio Bremen statt. U. a. hat sich der AK DSB auf der Sitzung mit einer technischen Einrichtung zur Messung von Zugriffen auf die Web-Angebote der Rundfunkanstalten befasst. Der AK DSB konnte sich davon überzeugen, dass dabei keine Permanent-Cookies eingesetzt werden. Die Auswertungen erfolgen anonym. Ein weiteres Thema war die ursprünglich geplante Grundverschlüsselung bei ASTRA. Diese Pläne sind aber inzwischen wieder aufgegeben worden. Weitere Themen waren: die Überarbeitung einer Datenschutzklausel in dem Vertrag mit dem von mehreren ARD-Anstalten beauftragten Reisebüro, die Modalitäten der Nutzungsmessung bei SAP, die geplante NP-Datenbank und das neue Historie-Löschkonzept der GEZ sowie das bei der GEZ praktizierte Verfahren im Zusam-

menhang mit der Bearbeitung von Anträgen auf Befreiung von der Rundfunkgebührenpflicht.

Am 23. August 2006 nahm ich als Mitglied der entsprechenden Unterarbeitsgruppe an einer Sitzung bei der GEZ in Köln zum neuen Löschkonzept in DV2005 teil. Zum Thema NP-Datenbank nahm ich als eine von mehreren Vertreterinnen und Vertretern des AK DSB am 31. 3. 2006 in Frankfurt und am 27. 4. 2006 in Stuttgart an gemeinsamen Sitzungen mit den Leiterinnen und Leitern der Abteilung Rundfunkgebühren teil.

Art. 29 Abs. 2 der EU-Datenschutzrichtlinie sieht die Einsetzung einer Europäischen Datenschutzgruppe vor, die aus Vertretern der einzelnen Mitgliedstaaten der EU besteht. Unter dem Vorsitz des Bundesbeauftragten für den Datenschutz, Herrn Peter Schaar, berät sie die EU-Kommission und trägt zur einheitlichen Anwendung der Datenschutzrichtlinie der EU-Staaten bei. Seit Ende 2001 ist ein Vertreter des AK DSB, der Datenschutzbeauftragte des NDR, Herr Maximilian Merten, an der Arbeit der Gruppe beteiligt.

## **II. IT-Sicherheitsgremium für das ARD-Corporate Network**

Das IT-Sicherheitsgremium für das Corporate Network (CN) der ARD verantwortet den Datensicherheitsprozess im gemeinsamen Datennetz der ARD-Anstalten. Einhergehend damit werden Applikationen und Dienste von dem Gremium vor dem Einsatz im CN sicherheitstechnisch bewertet. Für damit die zusammenhängenden datenschutzrechtlichen Fragestellungen und als Verbindungsstelle zum AK DSB vertrete ich den AK DSB als ständiges beratendes Mitglied in dem IT-Sicherheitsgremium.

Im Berichtszeitraum hat das Gremium dreimal getagt:

Die Sitzungen fanden am 31. 5. 2006 beim MDR in Dresden, am 11. 10. 2006 beim SWR in Baden-Baden und am 31. 1. 2007 beim BR in München statt. Themen waren unter anderem der geplante Video-Filetransfer im ARD-CN, Mindeststandards für

die IT-Sicherheit für mobile Produktionsnetzwerke, die Behandlung von Sicherheitsvorfällen und die gemeinsame Anschaffung eines IT-Sicherheitsinformationssystems.

### **III. Teilnahme an Veranstaltungen**

Am 19. 9. 2006 und am 21. 2. 2007 habe ich gemeinsam mit dem Vorsitzenden des AK DSB, Herrn Drescher, als Gast an der Sitzung des Arbeitskreises Medien der staatlichen Datenschutzbeauftragten in Klein Machnow bzw. Potsdam teilgenommen. Die Landesdatenschutzbeauftragte von Brandenburg, Frau Dagmar Hartge, ist Vorsitzende des Arbeitskreises. Themen waren u.a. die Neuordnung der Rundfunkfinanzierung, das Verfahren zur Befreiung von der Rundfunkgebührenpflicht, die geplante Vorratsdatenspeicherung in der elektronischen Kommunikation sowie die datenschutzrechtlichen Aspekte des Urheberrechts bei der Nutzung des Internets.

Am 4. Juli 2006 habe ich an der Fachkonferenz der Friedrich-Ebert-Stiftung zum Thema „Herausforderungen des Datenschutzes in der großen Koalition“ in Berlin teilgenommen. U. a. ging es dabei um die geplante Vorratsdatenspeicherung der Telekommunikations-Verbindungsdaten.

Berlin, 25. Juni 2007

gez. Anke Naujock