

# **5. Tätigkeitsbericht**

der Beauftragten für den Datenschutz  
des Rundfunk Berlin-Brandenburg

## **Berichtszeitraum:**

**1. April 2007 bis 31. März 2008**

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

## Inhaltsverzeichnis

	<u>Seite</u>
Vorbemerkung	5
<b>A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg</b>	<b>7</b>
I.    Gesetzliche Grundlagen	7
II.   Konkrete Situation	8
<b>B. Entwicklung des Datenschutzrechts</b>	<b>8</b>
I.    Europa	8
1.    Gesetzgebung	8
1.1    Europäische Verordnung zur Überwachung von Bargeld	8
1.2    Abkommen der EU mit den USA wegen Fluggastdaten	9
2.    Rechtsprechung	10
Klage der EU-Kommission gegen die Bundesrepublik Deutschland wegen unzureichender Umsetzung der EG-Datenschutzrichtlinie	
II.   Bund	11
1.    Gesetzgebung	11
1.1    10. Rundfunkänderungsstaatsvertrag	11
1.2.   Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG	13
2.    Rechtsprechung	15
Urteil des BVerfG vom 27.2.2008 zur Online-Durchsuchung (1 BvR 370/07 und 1 BvR 595/07)	
<b>C. Datenschutz und Datensicherheit im rbb</b>	<b>17</b>
I.    Aktuelle IT-Projekte	17
1.    Neues Dispositionssystem	17
2.    Rechtemanagementsystem (RMS)	17
3.    Urlaubs- und Fehlzeitenverwaltungssystem	18
4.    Bewerbermanagementsystem	20

	<u>Seite</u>	
II.	Datenschutz beim Online-Angebot des rbb	22
	1. Speicherung von IP-Adressen	22
	2. Datenschutz bei MeinFritz.de	23
III.	Arbeitnehmerdatenschutz in der Personalwirtschaft	24
	1. Betriebliches Eingliederungsmanagement (BEM)	24
	2. Auswertungen Krankheitstage	26
	3. Neuer Tarifvertrag für arbeitnehmerähnliche Personen des Rundfunk Berlin-Brandenburg	27
IV.	Sonstiges	27
	1. Reuters Mediendienste	27
	2. Löschrufen bei SAP	28
	3. Webcam der streamcast media GmbH auf dem Alexanderplatz	29
	4. Diverse Einzelvorgänge	30
V.	Informationsmaßnahmen	30
	1. Datenschutzrechtliche Schulung der Rundfunkgebühren- beauftragten	30
	2. Datenschutzrechtliche Schulung der Auszubildenden	31
<b>D.</b>	<b>Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung</b>	<b>31</b>
I.	Allgemeines	31
II.	Anfragen und Auskunftersuchen	32
III.	np-Datenbank	34
IV.	Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Bremen, Hessen, Berlin und Brandenburg	34
<b>E.</b>	<b>Datenschutz im Informationsverarbeitungszentrum (IVZ)</b>	<b>35</b>
I.	Allgemeines	35
II.	Spezielles	35
	1. Neue Hörfunkdatenbank	35
	2. Kein Einsatz des SAP-Solution Managers	36
	3. Neues von den Teleheimarbeitsplätzen	36
	4. BSI-Zertifizierung	37
<b>F.</b>	<b>Datenschutz im ARD-Hauptstadtstudio (HSB)</b>	<b>38</b>
<b>G.</b>	<b>Sonstiges</b>	<b>38</b>
I.	Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR	38
II.	IT-Sicherheitsgremium für das ARD-Corporate Network	39

	<u>Seite</u>
III. Arbeitskreis Medien der Staatlichen Datenschutzbeauftragten	40
IV. Gespräch mit Vertretern des LDSB Brandenburg und des BerIDSB	40
V. Teilnahme an Veranstaltungen	41
1. Internationales Symposium zum Thema „Datenschutz beim digitalen Fernsehen“	41
2. 2. Europäischer Datenschutztag	41

## Vorbemerkung

Mit diesem Tätigkeitsbericht möchte ich einen Überblick über meine Arbeit in dem Zeitraum 1. April 2007 bis 31. März 2008 geben. Der Bericht umfasst sowohl meine Aktivitäten als Datenschutzbeauftragte für den journalistisch-redaktionellen Bereich gemäß § 38 **rbb**-Staatsvertrag als auch meine Betätigung als sog. behördliche Datenschutzbeauftragte gemäß § 19 a Berliner Datenschutzgesetz (BerIDSG). Ich veröffentliche meine Tätigkeitsberichte im Online-Angebot des **rbb** unter der Adresse: <http://www.rbb-online.de>.

Einen Schwerpunkt bildete die Beobachtung der Gesetzgebung. Die mit den zusätzlich eingeführten präventiven Sicherheitsmaßnahmen einhergehende Einschränkung der Privatsphäre trifft alle Bürgerinnen und Bürger. Bei den im Berichtszeitraum beschlossenen Eingriffsbefugnissen fällt aber auf, dass auch die Journalistinnen und Journalisten zunehmend von Überwachungsmaßnahmen betroffen sind. Beispielhaft ist hier die Vorratsdatenspeicherung in der Telekommunikation zu nennen, bei der es - wie auch für andere Berufsheimnisträger - keine Sonderregelung für Journalisten gibt. Dadurch sind das Redaktionsgeheimnis und der Informantenschutz ernsthaft gefährdet.

Innerhalb des **rbb** war ich wieder hauptsächlich mit Fragen des Arbeitnehmerdatenschutzes befasst. Meine Aufgabe ist es, immer wieder die Frage nach der Erforderlichkeit und Verhältnismäßigkeit neuer Möglichkeiten der elektronischen Verarbeitung der Mitarbeiter-Daten zu stellen. Erfreulicherweise ist den Verantwortungs-trägern der Grundsatz der Datensparsamkeit bei der Planung neuer Vorhaben in den meisten Fällen schon von vornherein bewusst.

Ein besonderes Augenmerk habe ich auch im Berichtszeitraum wieder auf einen effektiven Rundfunkteilnehmerdatenschutz gelegt. Gerade unter dem Aspekt der Gebührenlegitimation und Gebührenakzeptanz des öffentlich-rechtlichen Rundfunks ist es wichtig, dass sich die Rundfunkteilnehmerinnen und -teilnehmer sicher sein können, dass der Datenschutz beim Rundfunkgebühreneinzug gewährleistet ist.

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

Der Datenschutz ist im Bewusstsein der meisten **rbb**-Mitarbeiterinnen und -Mitarbeiter fest verankert. Die Einbeziehung der Datenschutzbeauftragten in neue Vorhaben und Projekte mit datenschutzrechtlicher Relevanz auf der Grundlage der Datenschutz-Dienstanweisung ist erfreulicherweise zur Routine geworden und wird von keiner Seite mehr infrage gestellt.

Bei dem Systemverantwortlichen für IT-Sicherheit, Herrn Gerry Wolff, möchte ich mich wieder für die gute Zusammenarbeit im zurückliegenden Jahr bedanken. Ohne seine Unterstützung wäre ich oftmals nicht in der Lage gewesen, die technischen Aspekte eines Sachverhalts richtig einzuschätzen.

## **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/ihres 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 28. Juni 2007 hat mich der Rundfunkrat gemäß § 38 Abs. 1 **rbb**-Staatsvertrag auf Vorschlag der Intendantin einstimmig für eine weitere Amtszeit von vier Jahren zur Beauftragten für den Datenschutz des **rbb** bestellt.

Parallel dazu hat mich die Intendantin für den gleichen Zeitraum mit der Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten im Sinne von § 19 a BlnDSG beauftragt. Meine Funktion als Datenschutzbeauftragte des **rbb** nehme ich nebenamtlich zu meiner Tätigkeit im Justitiariat wahr. Eine Stellvertretung für die behördliche Datenschutzbeauftragte ist nach wie vor nicht bestellt.

Die datenschutzrechtliche Kontrolle durch den Berliner Landesdatenschutzbeauftragten in Abstimmung mit der Brandenburgische Datenschutzbeauftragten gemäß § 38 Abs. 8 **rbb**-Staatsvertrag beschränkte sich auch im Berichtszeitraum wieder auf die Einhaltung des Datenschutzes beim Rundfunkgebühreneinzug. Die Zusammenarbeit mit den Behörden ist konstruktiv und kollegial. In vielen Fragestellungen gibt es inhaltliche Übereinstimmungen in der datenschutzrechtlichen Bewertung, die einen gemeinsamen Einsatz in der Sache ermöglichen.

Diese positiven praktischen Erfahrungen ändern freilich nichts an meinem Rechtsstandpunkt, wonach die Aufspaltung der Kontrollkompetenzen, die es vergleichbar außer beim **rbb** nur noch beim Hessischen Rundfunk und bei Radio Bremen gibt, verfassungsrechtlich zumindest bedenklich ist.

## B. Entwicklung des Datenschutzrechts

### I. Europa

#### 1. Gesetzgebung

##### 1.1 Europäische Verordnung zur Überwachung von Bargeld

Europäische Verordnungen wirken wie (deutsche) Gesetze unmittelbar gegenüber allen Bürgern (und nicht nur mittelbar wie Richtlinien). Seit dem 15. Juni 2007 gilt

die „Verordnung (EG) Nr. 1889/2005 über die Überwachung von Barmitteln, die in die Gemeinschaft oder aus der Gemeinschaft verbracht werden“ (Amtsblatt EU vom 25.11.2005, L 309/9). Erfasst werden alle Personen, die in die EU einreisen oder ausreisen und dabei Barmittel (z.B. Bargeld oder Schecks) in Höhe von 10.000 € oder mehr mit sich führen. Sie sind verpflichtet, auch ohne Aufforderung eine selbstständige schriftliche Anzeige zu machen und dabei anzugeben: Anmelder (Name, Geburtsdaten, Staatsangehörigkeit), Eigentümer und Empfänger des Geldes, Herkunft und Verwendungszweck sowie Reiseweg und Verkehrsmittel. Da die Regelungen ohne Ausnahmen gelten, müssen auch Journalistinnen und Journalisten, wenn sie Barmittel für eine Aktivität im Ausland (z.B. eine Reportage) mitnehmen, diese Verpflichtungen erfüllen.

## **1.2. Abkommen der EU mit den USA wegen Fluggastdaten**

Nachdem der Europäische Gerichtshof (EuGH) eine Vereinbarung zwischen der EU und den Vereinigten Staaten von Amerika zur Übermittlung und Verwendung von Fluggastdaten (sog. PNR-Abkommen) mit Urteil vom 30. Mai 2006 aus formellen Gründen für rechtswidrig angesehen hatte, schlossen die Parteien am 26. Juli 2007 eine neue Übereinkunft. Sie wurde vom Bundestag ohne große Debatte mit Gesetz vom 20. Dezember 2007 gebilligt und in deutsches Recht umgesetzt (BGBl. II, 2007, 1978 ff.). Der Zweck dieses sog. PNR-Abkommens (*Passenger Name Records*) liegt in der Verhütung und Bekämpfung von „Terrorismus und damit zusammenhängender Straftaten“ sowie „sonstiger schwerer Straftaten grenzüberschreitender Art“ (einschl. der organisierten Kriminalität). Dazu können eine Vielzahl von Daten über den Reisenden (und Mitreisende) und die Reise (bis hin zum Sachbearbeiter des Reisebüros) erhoben und weitergegeben werden. Die Daten werden sieben Jahre „in einer aktiven analytischen Datenbank“ gespeichert und dann für weitere acht Jahre aufbewahrt. Damit sind Flugbewegungen auch von Journalistinnen und Journalisten über Jahre hinweg nachvollziehbar und können ausgewertet und mit anderen Daten verknüpft werden.

## 2. Rechtsprechung

### **Klage der EU-Kommission gegen die Bundesrepublik Deutschland wegen unzureichender Umsetzung der EG-Datenschutzrichtlinie**

Im Vertragsverletzungsverfahren gegen Deutschland um die Einrichtung unabhängiger Datenschutzstellen hat die EU-Kommission mit Klage vom 22. November 2007 den EuGH angerufen. Die Klage nach Art. 226 Abs. 2 EG-Vertrag stützt sich auf Art. 28 Abs. 1 der Datenschutzrichtlinie (95/46/EG), der die „völlige Unabhängigkeit“ der die Umsetzung der Richtlinie überwachenden Behörden fordert. Die Kommission ist der Auffassung, dass dies bei den Länderbehörden, denen die Datenschutzaufsicht über private Stellen obliegt, nicht der Fall ist. Die Datenschutzbehörden unterstünden in allen 16 Bundesländern einer staatlichen Fach-, Rechts- bzw. Dienstaufsicht. Der Wortlaut der Richtlinie verlange aber, dass die Einflussnahme von außerhalb der Behörde ausgeschlossen sein müsse. „Völlige“ Unabhängigkeit im Wortsinne sei nur gewährleistet, wenn eine Abhängigkeit nicht nur von jeder Seite, sondern auch in jeder Hinsicht ausgeschlossen werden könne.

Dagegen hatte die Bundesregierung bislang stets argumentiert, die Richtlinie verlange lediglich eine funktionelle, nicht jedoch eine darüber hinausgehende organisatorische Unabhängigkeit. Das Demokratieprinzip und der Grundsatz der parlamentarischen Verantwortung der Regierung verlangten grundsätzlich die Weisungsgebundenheit der Verwaltung gegenüber der Regierung. Auch habe die Kommission keine Kompetenz, die Organisation des Verwaltungsaufbaus in den Mitgliedstaaten zu bestimmen. Maßgebend sei, dass die zu kontrollierenden Unternehmen und Bürger keinen Einfluss auf die Datenschutzbehörde haben dürfen. Dies sei in Deutschland gewährleistet.

Die Stellung der Rundfunkdatenschutzbeauftragten in Deutschland ist von dem Verfahren nicht unmittelbar tangiert.

## **II. Bund**

### **1. Gesetzgebung**

#### **1.1. 10. Rundfunkänderungsstaatsvertrag**

Am 19. Dezember 2007 haben die Regierungschefs der Länder den 10. Rundfunkänderungsstaatsvertrag (RÄndStV) unterzeichnet. Er soll nach Zustimmung aller Landesparlamente am 1. September 2008 in Kraft treten. Aus datenschutzrechtlicher Sicht sind folgende Änderungen hervorzuheben:

In § 6 Abs. 2 Rundfunkgebührenstaatsvertrag (RGebStV), der die Anforderungen an den Nachweis bei dem Antrag auf Rundfunkgebührenbefreiung enthält, wurde nun ausdrücklich die Möglichkeit der Vorlage einer entsprechenden Bestätigung des Leistungsträgers über den Bezug von Sozialleistungen aufgenommen. Der Hintergrund der Änderung des § 6 Abs. 2 RGebStV ist Folgender:

Mit der Reform des Befreiungsrechts im 8. RÄndStV wurden seinerzeit auch dessen formelle Voraussetzungen in § 6 Abs. 2 RGebStV festgelegt. Wer als private Person eine Befreiung begehrt, muss hierfür den vollständigen Nachweis des jeweiligen Sozialleistungsträgers erbringen. Dazu ist die Vorlage der entsprechenden Bescheide (z.B. über Grundsicherung, Sozialhilfe oder Arbeitslosengeld II) im Original oder in beglaubigter Kopie notwendig. In diesen teils umfänglichen Bescheiden sind zum Teil auch persönliche Daten enthalten, die für die Bearbeitung des Antrags auf Gebührenbefreiung nicht erforderlich sind.

Im Interesse einer konsequenten Datensparsamkeit erkennt die GEZ auch schon derzeit entsprechende Bescheinigungen der Sozialleistungsträger, die nur die für die Entscheidung über die Befreiung von der Rundfunkgebührenpflicht notwendigen Daten enthalten, an. Dieses Verfahren ist auf Empfehlung der jeweiligen datenschutzrechtlichen Kontrollinstanzen für den Gebühreneinzug, den Landes- und den Rundfunkdatenschutzbeauftragten, nun auf eine eindeutige gesetzliche Grundlage gestellt worden. Die angestrebte elektronische Übermittlung von Daten aller Leistungsträger an die GEZ wird aufgrund der technischen Schwierigkeiten nach Ein-

schätzung der GEZ frühestens ab 2010 flächendeckend zu realisieren sein. Erste Pilotprojekte mit einzelnen Behörden sind positiv ausgefallen.

Die Regelung des § 8 Abs. 4 RGebStV, die durch den 8. RÄndStV als bundesweit einheitliche Rechtsgrundlage für sogen. Mailingaktionen der GEZ eingeführt worden ist, wurde neu gefasst und verbessert.

§ 8 Abs. 4 Satz 1 RGebStV bildet die notwendige Rechtsgrundlage für die Datenverwendung zur Feststellung, ob ein Rundfunkteilnehmerverhältnis vorliegt und ermöglicht damit z.B. die Datenbeschaffung bei privatrechtlichen Adresshändlern und den danach erfolgenden Datenabgleich. Statt der bisherigen pauschalen Verweisung auf § 28 BDSG wird mit § 8 Abs. 4 Satz 2 RGebStV eine detaillierte rundfunkspezifische Regelung vorgenommen, in der die Voraussetzungen, unter denen personenbezogene Daten beschafft werden dürfen, konkretisiert werden. Mit der Streichung der Verweisung auf § 28 BDSG ist auch klargestellt, dass kein Widerspruchsrecht gegen eine Datenverwendung (z.B. nach § 28 Abs. 4 BDSG) besteht.

§ 8 Abs. 4 Satz 3 RGebStV zwingt die Landesrundfunkanstalten und die für sie handelnde GEZ, die von Dritten beschafften und gespeicherten personenbezogenen Daten innerhalb eines Jahres zu bearbeiten, da sie nach Ablauf dieser Frist zu löschen sind. Stellt sich bei der Bearbeitung heraus, dass kein Rundfunkteilnehmerverhältnis besteht, sind die erworbenen Daten nach § 8 Abs. 4 Satz 4 RGebStV unverzüglich zu löschen. Stellt sich heraus, dass ein Teilnehmerverhältnis begründet oder erweitert worden ist, so sind die erworbenen und sonstigen erforderlichen Daten in der Rundfunkteilnehmerdatenbank zu überführen und dürfen entsprechend dem Grundsatz der Zweckbindung nur dort gespeichert und verwendet werden. In der ursprünglichen Datenbank sind sie zu löschen.

Die Datenerhebung aus öffentlichen Registern oder aufgrund von melderechtlichen Normen ist wie bislang unabhängig von der Regelung des § 8 Abs. 4 RGebStV möglich.

## **1.2. Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG**

Unter anderem zur Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung in Deutsches Recht hat der Deutsche Bundestag das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen“ beschlossen. Es ist am 1. Januar 2008 in Kraft getreten. Neben den in das Telekommunikationsgesetz (TKG) eingefügten Regelungen zur Vorratsdatenspeicherung enthält das Gesetz auch Änderungen der Strafprozessordnung hinsichtlich der Verwendung dieser Daten sowie zu anderen verdeckten Ermittlungsmaßnahmen.

Nach dem neuen Gesetz besteht nunmehr für Anbieter, die öffentlich zugängliche Telekommunikationsdienste erbringen, eine Verpflichtung, die Verbindung aller Telefon- und Handy-Gespräche (Ausgangs- und Zielrufnummer, Verbindungsdauer, Datum) und die entsprechenden Daten bei der Internetkommunikation verdachts- und anlassunabhängig zu speichern. Bei Gesprächen unter Beteiligung eines Mobilgerätes werden außerdem die eindeutige 15-stellige Seriennummer (IMEI) des Gerätes und die jeweiligen Funkzellen (und damit die ungefähren Standorte der Telefonierenden) gespeichert. Diese Regelungen gelten auch für Fax- und SMS-Dienstleistungen. Die Speicherungspflicht nimmt auch Privatpersonen (beispielsweise, wenn sie kostenlos einen öffentlichen WLAN-Zugang anbieten) und Anonymisierungsdienste nicht aus.

Die Speicherdauer beträgt in allen Fällen mindestens sechs, maximal sieben Monate (vgl. § 113a TKG). Anbieter von Internetzugängen, Internet-Telefonie und E-Mail sind erst ab dem 1. Januar 2009 zur Speicherung verpflichtet; mehrere Provider haben angekündigt, diese Übergangsfrist wahrzunehmen.

Übermittelt werden müssen die Verbindungsdaten schon bei Verdacht von erheblichen Gefahren für die öffentliche Sicherheit und zur Erfüllung der gesetzlichen Aufgaben der Geheimdienste (BND, MAD, Verfassungsschutzbehörden). Die dem Gesetzespaket zugrunde liegende EU-Richtlinie sieht die Datenspeicherung hingegen nur zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren

Straftaten vor. Ebenso sind u. a. der Identifizierungszwang der Nutzer und die Speicherungspflicht bei Anonymisierungsdiensten in der EU-Richtlinie nicht vorgesehen. Damit geht das deutsche Gesetz weit über die EU-Vorgaben hinaus.

Vor Inkrafttreten des Gesetzes durften solche Daten nur solange gespeichert werden, wie der Nutzer dies erlaubt hat (bis zu 90 Tage) oder solange sie für Abrechnungszwecke benötigt wurden. Bisher benötigen die Strafverfolgungsbehörden einen „strafprozessualen Anfangsverdacht“, um ermitteln zu dürfen. Nun steht grundsätzlich jeder Bürger unter Generalverdacht.

Diese Regelungen ermöglichen nicht nur die Erstellung eines umfassenden Bildes der privaten und beruflichen Kommunikation jedes Bürgers, sondern über die Speicherung von IP-Adressen lassen sich die Interessen und Vorlieben von Bürgern nachvollziehen. Dies hat auch gravierende Auswirkungen auf die journalistische Praxis. Denn mithilfe der genannten Daten kann auch die gesamte berufliche Kommunikation von Journalisten nachvollzogen werden. Die Speicherung aller Telefon- und Handyverbindungen sowie Internetzugriffe über sechs Monate stört die auf Vertrauen basierende Beziehung zwischen Journalist und Informant deutlich und kann Quellen versiegen lassen. Damit wird ein seriöser, investigativer Journalismus, der auf eine vor äußeren Eingriffen geschützte Informationsbeschaffung angewiesen ist, im Kern getroffen. Das gilt umso mehr, wenn man die erweiterten Verwendungsmöglichkeiten bedenkt, die den Strafverfolgungsbehörden nach §§ 97 ff StPO eingeräumt werden.

Zwar ist gegen die dem Gesetz zugrunde liegende Richtlinie ein Verfahren vor dem Europäischen Gerichtshof anhängig, das - unter Berücksichtigung der bisherigen Rechtsprechung des EuGH in vergleichbaren Fällen - vermutlich dazu führen wird, dass die Richtlinie für europarechtswidrig erklärt werden wird. Allerdings würde dies keine Auswirkungen auf die Geltung der jetzt beschlossenen Regelungen haben.

Der Arbeitskreis Vorratsdatenspeicherung - ein bundesweiter Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern - hat gegen das Gesetz

eine Verfassungsbeschwerde eingereicht, für die Vollmachten von über 34.000 Beschwerdeführern vorliegen und die damit als die größte Verfassungsbeschwerde in der Geschichte der Bundesrepublik gilt.

Über den der Klage beigefügten Eilantrag, mit dem eine sofortige Aussetzung des Gesetzesvorhabens durch einstweilige Anordnung bis zur Entscheidung in der Hauptsache gefordert worden ist, hat das Bundesverfassungsgericht (BVerfG) am 19. März 2008 entschieden und ihm teilweise stattgegeben. Danach ist die Übermittlung der gespeicherten Telekommunikationsdaten an Strafverfolgungsbehörden vorläufig nur für diejenigen Ermittlungsverfahren zugelassen, die eine schwere Straftat im Sinne des § 100 a Abs. 2 STPO zum Gegenstand haben, die auch im Einzelfall schwer wiegt, bei denen der Verdacht durch gestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre. Darüber hinaus muss die Bundesrepublik dem BVerfG über die praktischen Auswirkungen der Datenspeicherungen und der vorliegenden einstweiligen Anordnung berichten. Die Einschränkung gilt vorläufig für sechs Monate. Es bleibt abzuwarten, wie das BVerfG in der Hauptsache entscheiden wird.

## **2. Rechtsprechung**

### **Urteil des BVerfG vom 27. 2. 2008 zur Online-Durchsuchung (1 BvR 370/07 und 1 BvR 595/07)**

Einem Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 (Az. 1 BvR 370/07 und 1 BvR 595/07) zufolge dürfen Computer von Personen, die einer Straftat verdächtig sind, nur dann mit Spionagesoftware ausgeforscht werden, wenn dies zum Schutz überragend wichtiger Allgemeingüter erforderlich ist.

In dem Urteil erklärte das BVerfG die in dem Verfassungsschutzgesetz des Landes Nordrhein-Westfalen (VSG) enthaltene Rechtsgrundlage zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“) für verfassungswidrig und nichtig.

Nach Ansicht des BVerfG stellt die Online-Durchsuchung einen Eingriff in das nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz geschützte allgemeine Persönlichkeitsrecht dar. Es führte dazu aus, dass die Nutzung informationstechnischer Systeme, insbesondere von Personalcomputern, eklatante Wichtigkeit für die Persönlichkeitsentfaltung vieler Bevölkerungsschichten erlangt habe. Insbesondere das Internet sei von herausragender Bedeutung für die Entfaltung der Persönlichkeit, da es nicht nur eine unübersehbare Fülle von Informationen bereitstelle, sondern auch zahlreiche neue Kommunikationsdienste, mit deren Hilfe der Nutzer aktiv soziale Kontakte aufbauen und pflegen könne. Dadurch würden gleichzeitig aber auch neue Gefährdungen für das allgemeine Persönlichkeitsrecht begründet. Denn eine Überwachung der Nutzung solcher Systeme und die Auswertung ihrer Daten könnten weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers ermöglichen.

Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgte das BVerfG ein grundrechtlich erhebliches Schutzbedürfnis und formulierte ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ als besondere Ausprägung des allgemeinen Persönlichkeitsrechts. Zwar, so betont das BVerfG, könnten Eingriffe in dieses Grundrecht sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Das VSG genüge im vorliegenden Fall aber nicht den verfassungsrechtlichen Anforderungen an eine gesetzliche Grundlage für einen derartigen Eingriff. So sei die heimliche Infiltration eines informationstechnischen Systems, mit deren Hilfe die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut (etwa Leib, Leben und Freiheit der Person) bestünden. Zudem verlangt das Gericht, den heimlichen Zugriff auf informationstechnische Systeme unter den Vorbehalt richterlicher Anordnung zu stellen, und Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

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

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

#### **1. Neues Dispositionssystem**

Wie in meinem letzten Tätigkeitsbericht bereits erwähnt, arbeitet eine Projektgruppe an der Einführung eines neuen gemeinsamen Dispositionssystems für Hörfunk und Fernsehen, mit dessen Unterstützung zukünftig Personal und Sachmittel im **rbb** einheitlich disponiert werden sollen.

Im Rahmen eines Vorprojektes waren zunächst die unterschiedlichen Prozesse in Hörfunk und Fernsehen aufgenommen worden. Auf Basis dieser Ergebnisse, einer Marktanalyse und Berücksichtigung optimierter Geschäftsprozesse erfolgte die Erstellung des Leistungsverzeichnisses, in das auch die von mir definierten Anforderungen an Datenschutz und Datensicherheit eingeflossen sind. Nach Angebotsprüfung erhielten im Juni 2007 die Firmen GISA und CEITON den Auftrag. Nach Beauftragung der Firmen wurde mit ihnen zusammen die Feinkonzeption durchgeführt. Das Feinkonzept/Pflichtenheft beschreibt Änderungen an der schon existierenden Produktversion im Rahmen des **rbb**-Projektes, z. B. Änderungen an Masken, Funktionen und Schnittstellen zu Drittsystemen. In dem Feinkonzept sind alle meine datenschutzrechtlichen Forderungen berücksichtigt worden. Das betrifft insbesondere ein detailliertes Berechtigungskonzept.

Über die Einführung und Nutzung des Dispositionssystems wird voraussichtlich eine Dienstvereinbarung mit dem Personalrat abgeschlossen werden. An den Verhandlungen über die Dienstvereinbarung werde ich beteiligt.

#### **2. Rechtemanagementsystem (RMS)**

In meinem letzten Tätigkeitsbericht hatte ich über die Einführung des neuen Rechtemanagementsystems (RMS) beim **rbb** im Herbst 2006 berichtet. Vor der Einführung war es mir nicht möglich gewesen, eine abschließende datenschutzrechtliche

Bewertung des Systems vorzunehmen, da mir die notwendigen Unterlagen nicht rechtzeitig vorgelegt worden waren. Auf der Grundlage der seinerzeit bereits vorliegenden Informationen hatte ich dem Probetrieb ab Herbst 2006 zustimmen können. Erst nach Veröffentlichung meines Tätigkeitsberichts habe ich erfahren, dass am 30. März 2007 eine Dienstvereinbarung mit dem Personalrat abgeschlossen worden war, die sich in ihrem Aufbau eng an die Dienstvereinbarungen für die anderen SAP-Module, die unter meiner Mitwirkung zustande gekommen sind, anlehnt.

### **3. Urlaubs- und Fehlzeitenverwaltungssystem**

Im Sommer 2008 soll im **rbb** ein Urlaubs- und Fehlzeitenverwaltungssystem eingeführt werden. Ziel ist es, die Abwesenheitsinformationen bereits am Entstehungsort elektronisch zu erfassen und anschließend automatisiert an das Personaldatenverarbeitungssystem SAP/HR zu übergeben. Alle fest angestellten Mitarbeiterinnen und Mitarbeiter erhalten im System ein Abwesenheitsinformationskonto. Die Mitarbeiterstammdaten werden aus SAP/HR übernommen. Die Mitarbeiterinnen und Mitarbeiter sollen ihre Urlaubsanträge und Anträge auf Arbeitsbefreiung, die bislang auf entsprechenden Papierformularen gestellt und nach Genehmigung durch die Vorgesetzten von der HA Personal in SAP eingegeben werden, zukünftig selbst in das elektronische System eingeben. Das Genehmigungsverfahren soll auf elektronischem Weg und die Übergabe der Urlaubs-/Arbeitsbefreiungsdaten an SAP/HR automatisch erfolgen. Fehl- und Rückmeldungen sollen ebenfalls elektronisch im Urlaubs- und Fehlzeitenverwaltungssystem durchgeführt und die entsprechenden Daten automatisch an SAP/HR übergeben werden. Alle Mitarbeiterinnen und Mitarbeiter können sich dann im Urlaubs- und Fehlzeitenverwaltungssystem jederzeit über ihren Resturlaub sowie über den Genehmigungsstatus ihrer Anträge informieren. Die jeweiligen Vorgesetzten können sich jederzeit über die An- und Abwesenheitszeiten ihrer Mitarbeiterinnen und Mitarbeiter informieren. Das reduziert entsprechende Anfragen in der HA Personal und entlastet die dortigen Kolleginnen und Kollegen.

Nach erfolgreicher Durchführung meiner datenschutzrechtlichen Vorabkontrolle des Systems zusammen mit dem Systemverantwortlichen für IT-Sicherheit haben Intendantin und Personalrat eine Dienstvereinbarung über die Anwendung des Systems abgeschlossen. In die Dienstvereinbarung sind alle meine Forderungen zu Datenschutz und Datensicherheit eingeflossen.

Es werden nur diejenigen personenbezogenen Daten der Kolleginnen und Kollegen mit dem System verarbeitet, die für die Abwicklung von Urlaub und anderen Fehlzeiten erforderlich sind. Die Auswertungsmöglichkeiten sind wie die Zugriffsrechte sehr eingeschränkt. Auch die Aufbewahrungsfristen sind detailliert in der Dienstvereinbarung geregelt.

Bedenken hatte ich hinsichtlich der Option, eine Vertreterregelung zu treffen. Danach können die Mitarbeiterinnen und Mitarbeiter andere Kollegen mit der Erfassung ihrer Urlaubsanträge und Anträge auf Arbeitsbefreiung beauftragen. Die Konsequenz ist, dass die beauftragte Person Einblick in deren gesamte Urlaubshistorie (einschließlich Sonderurlaub wegen besonderer Ereignisse) erhält. Ich hatte die Erforderlichkeit einer Vertreterregelung bezweifelt, da ja jede Mitarbeiterin/jeder Mitarbeiter die Möglichkeit hat, ihr/sein Urlaubskonto persönlich an einem PC (entweder dem persönlich zugeordneten oder an einem der Gruppen-PC) zu bearbeiten. Für den Fall des Festhaltens an der Vertreterregelung hatte ich gefordert, dass zumindest die Möglichkeit der Einsichtnahme in die Urlaubshistorie durch die beauftragten Dritten beschränkt wird.

Der Projektleiter hat mir daraufhin erläutert, dass es nach Information der Fachbereiche u. a. für Kolleginnen und Kollegen, die überwiegend extern tätig sind, und für Urlaubsanträge aus einer Abwesenheit heraus (Krankheit, Kur, Urlaub) die Möglichkeit einer Vertreterregelung geben muss. Er hat mir auch die Nachteile erläutert, die ein beschränkter Zugriff auf die Urlaubshistorie für die beauftragten Dritten mit sich gebracht hätte: Die Beauftragten hätten in diesem Fall nicht mehr den Status der von ihnen im Auftrag versendeten Anträge verfolgen können, d. h. sie hätten keine Rückmeldung, ob und wann der Antrag genehmigt oder abgelehnt worden ist, erhalten. Die Beauftragten hätten die im Auftrag versendeten Anträge nachträglich

auch nicht mehr ändern oder stornieren können. Außerdem wären sie gegenüber ihren Auftraggebern nur eingeschränkt auskunftsfähig gewesen.

Diese Argumentation überzeugte mich zwar nicht vollends. Angesichts der Tatsachen, dass jede Kollegin und jeder Kollege aber letztlich ja selbst entscheiden kann, ob überhaupt Dritte für sie/ihn Urlaube und Arbeitsbefreiungen beantragen dürfen und falls ja, wen sie/er damit beauftragen, habe ich die Regelung schließlich akzeptiert.

#### **4. Bewerbermanagementsystem**

Schon in meinem letzten Tätigkeitsbericht habe ich berichtet, dass beim **rbb** ein elektronisches Bewerbermanagementsystem eingeführt werden soll.

Im September 2007 hat die Geschäftsleitung nun beschlossen, das System HRECONNECT anzuschaffen. Damit können Stellenanzeigen im Internet publiziert werden, die Bewerberinnen und Bewerber können sich online bewerben und die elektronischen Bewerbungen können elektronisch weiterverarbeitet werden. Schriftliche Bewerbungen werden von der HA Personal in das System eingepflegt.

Die Umstellung soll zunächst in eingeschränktem Rahmen erfolgen: Im ersten Schritt werden nur Bewerbungen auf Praktikanten- und Ausbildungsplätze sowie auf studentische Aushilfstätigkeiten elektronisch verwaltet. Auch Bewerbungen per Post werden weiterhin akzeptiert. Die Möglichkeit einer automatischen Aussonderung (und Absage) wird nicht genutzt. Die HA Personal wird sich auch weiterhin jede Bewerbung ansehen. Wenn sich das System bewährt, soll es in einem zweiten Schritt auch auf sonstige Bewerbungen Anwendung finden.

Nach erfolgreicher Durchführung einer datenschutzrechtlichen Vorabkontrolle durch mich haben Geschäftsleitung und Personalrat im Frühjahr 2008 eine Dienstvereinbarung über die Nutzung des Systems abgeschlossen. In Kürze soll das System beim **rbb** implementiert werden.

Hervorzuheben ist, dass HReCONNECT in dem Rechenzentrum des Herstellers betrieben wird. Zusammen mit dem Systemverantwortlichen für IT-Sicherheit habe ich mich davon überzeugen können, dass bei der Datenübertragung die gängigen Datensicherheitsmaßnahmen (insbesondere Verschlüsselung) ergriffen werden. Elektronische Dokumente, die Bewerberinnen und Bewerber als Anlagen zu Bewerbungen im System speichern, werden automatisch in PDF-Dateien umgewandelt. Dadurch wird die Virenfreiheit und Revisionsicherheit der Dokumente gewährleistet. Die Authentifizierung der Nutzer des Systems (Bewerberinnen und Bewerber, Sachbearbeiter der HA Personal und der zuständigen Fachabteilungen) erfolgt datenbankbasiert. Dabei werden der Benutzername und ein Kennwort abgefragt.

Bei der Festlegung der von den Bewerbern auszufüllenden Pflichtfelder habe ich darauf geachtet, dass diese AGG (=Allgemeines Gleichbehandlungsgesetz) konform sind und sich an dem Grundsatz der Datensparsamkeit orientieren. Vor der Bewerbung müssen die Bewerberinnen und Bewerber ausdrücklich ihr Einverständnis dazu erteilen, dass der **rbb** ihre Bewerbungsdaten elektronisch verarbeiten darf. Das gilt auch bei Bewerbungen, die in Papierform eingehen, da die darin enthaltenen Informationen von der HA Personal zur weiteren Bearbeitung ebenfalls in HReCONNECT erfasst werden.

Sofern mit den Bewerbern nichts anderes vereinbart ist, wird nach Abschluss des Stellenbesetzungsverfahrens allen Systemnutzerinnen und -nutzern außer den Administratoren der Zugriff auf die Bewerbungsdaten entzogen. Die Bewerbungsdaten werden bis Ende des dritten Jahres nach Abschluss des Stellenbesetzungsverfahrens als Beweismittel für eventuelle Klagen gegen die Stellenbesetzung aufbewahrt und anschließend durch die Administratoren gelöscht.

Wie bei allen IT-Projekten habe ich auf ein schlüssiges Berechtigungskonzept geachtet. Die Protokollierungen im System sind in der Dienstvereinbarung abschließend geregelt. Die Protokolle stellen die in § 5 Abs. 2 Ziff. 5 BlnDSG geforderte Revisionsfähigkeit bei der Verarbeitung personenbezogener Daten sicher. Sie dürfen nur zur Systemwartung und - auf Anforderung der HA Personal und unter Einbeziehung des Personalrats und der Datenschutzbeauftragten - zum Nachweis der

ordnungsgemäßen Durchführung des Stellenbesetzungsverfahrens eingesehen werden. Ausdrücklich ausgeschlossen ist die Nutzung der Protokolle zur Leistungs- und Verhaltenskontrolle von Mitarbeiterinnen und Mitarbeitern.

## **II. Datenschutz beim Online-Angebot des rbb**

Im Sommer 2007 habe ich mich intensiv mit den datenschutzrechtlichen Fragestellungen im Zusammenhang mit dem Online-Angebot des **rbb** beschäftigt. Dabei habe ich sowohl die Verarbeitung der Nutzerdaten, die sog. IP-Daten, als auch die Verarbeitung der personenbezogenen und -bezieharen Inhaltsdaten näher betrachtet.

### **1. Speicherung von IP-Adressen**

Grundsätzlich dürfen gem. § 15 Abs. 1 Telemediengesetz (TMG) Nutzerdaten im Zusammenhang mit einem Telemedien-Angebot nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Zu den Nutzerdaten i. S. dieser Vorschrift gehört auch die IP-Adresse (statische und dynamische IP-Adresse). Da die vom **rbb** angebotenen Dienste allesamt kostenlos sind, bedarf es keiner Speicherung der IP-Adresse zu Abrechnungszwecken. Von den Mitarbeitern aus der IT-Abteilung wurde mir dazu allerdings mitgeteilt, dass eine befristete Speicherung der IP-Adressen aus Sicherheitsgründen unverzichtbar sei. Eine nähere Befassung mit dem Thema ergab, dass es einerseits zwar Rechtsprechung gibt, nach der die Speicherung von IP-Adressen für andere als für Abrechnungszwecke generell unzulässig ist (vgl. dazu Urteil des Amtsgerichts Mitte vom 27. 3. 2007, 5 C 314/06, bestätigt durch Landgericht Berlin, Anerkenntnis- und Schlussurteil vom 6.9.2007, 23 S 3/07), andererseits aber von zahlreichen Datenschutzrechtsexperten, z. B. auch von den meisten staatlichen Datenschutzbeauftragten, eine kurzfristige Speicherung zu Datensicherheitszwecken für zulässig erachtet wird.

Da es innerhalb der ARD eine einheitliche Lösung geben sollte, habe ich das Thema in den Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschland-

radio (AK DSB) eingebracht. Zur Aufklärung des Sachverhaltes hat der AK DSB das IT-Sicherheitsgremium für das ARD-CN (corporate network) um eine detaillierte Stellungnahme zur Notwendigkeit der Speicherung der IP-Daten gebeten. Nach dessen Einschätzung ist eine Protokollierung zur Gewährleistung des ordnungsgemäßen Betriebes von IT-Systemen sowie zur Abwehr von Angriffen aus dem Internet zwingend erforderlich. Die IP-Adressen würden zur Fehleranalyse und Fehlerbeseitigung benötigt und dienen der Angriffs-, Manipulations- und Missbrauchserkennung. Noch nicht abschließend geklärt ist die Dauer der notwendigen Speicherung. Das IT-Sicherheitsgremium plädiert für eine Speicherung von 30 Tagen. Diese Frist erscheint dem AK DSB zu lang. Der AK DSB befindet sich mit dem IT-Sicherheitsgremium diesbezüglich weiter im Dialog.

## **2. Datenschutz bei MeinFritz.de**

Schon seit geraumer Zeit ist das Internet nicht mehr nur eine Einbahnstraße, über die Websurfer Informationen abrufen können. Zunehmend werden die Nutzer selbst zu Anbietern von Informationen und gestalten Webseiten und deren Inhalte aktiv mit. Diese Entwicklung wird mit dem Schlagwort „Web 2.0“ bezeichnet und fasst eine Reihe verschiedener interaktiver und kooperativer Techniken bei der Nutzung des Internet zusammen.

Die hohe Attraktivität der Internetplattformen für soziale Netze liegt zunächst darin, dass jeder Nutzer selbst relativ einfach Webseiten mit persönlichen Informationen erstellen und veröffentlichen kann (so genannte Profile). Diese Selbstportraits enthalten häufig private Daten (Alter, Wohnort, Tätigkeit, Interessen, Freizeitaktivitäten und Kontaktmöglichkeiten) und werden ergänzt durch Fotos und Videos der Nutzer. Studien haben ergeben, dass ca. ein Viertel der Jugendlichen im Alter zwischen 12 und 19 Jahren in Deutschland auf diese Weise im Internet präsent sind.

Es wundert daher nicht, dass auch die Jugendwelle Fritz diese attraktive Möglichkeit der Hörerbindung nutzt. Fritz hat die Plattform MeinFritz.de eröffnet. Sie wird - wie vergleichbare Plattformen der Jugendhörfunkwellen von hr und mdr - auf einem Server beim MDR betrieben. Zwar existieren bereits ausführliche Nutzerbedin-

gungen, die auch einen datenschutzrechtlichen Teil enthalten. Ich halte es jedoch für erforderlich, die datenschutzrechtlichen Rahmenbedingungen noch konkreter als bisher zu definieren und auch die Nutzerbedingungen in dieser Hinsicht noch zu optimieren. Ich sehe hier die öffentlich-rechtlichen Anbieter in einer besonderen Verantwortung. Die Plattformen müssen mit ausführlichen Hinweisen und ausdrücklichen Einwilligungserklärungen zur Verarbeitung der Daten ausgestattet sein. Schon die Anzahl der Pflichteingabefelder muss so gering wie möglich gehalten werden. Ebenso muss das Agieren unter einem Pseudonym möglich sein.

Inzwischen habe ich dieses Thema auch mit meinen Kolleginnen und Kollegen im AK DSB erörtert. Sie teilen meine Auffassung. Zur Erarbeitung einheitlicher datenschutzrechtlicher Rahmenbedingungen wurde eine Arbeitsgruppe unter meinem Vorsitz gegründet. Die Arbeitsgruppe wird demnächst ihre Arbeit aufnehmen.

### **III. Arbeitnehmerdatenschutz in der Personalwirtschaft**

#### **1. Betriebliches Eingliederungsmanagement (BEM)**

Seit dem 1. Juli 2004 verpflichtet die Präventionsvorschrift des § 84 Abs. 2 Sozialgesetzbuch (SGB) IX alle privaten und öffentlichen Arbeitgeber zum sog. betrieblichen Eingliederungsmanagement (BEM), sobald ein Arbeitnehmer länger als sechs Wochen ununterbrochen oder wiederholt innerhalb eines Jahres arbeitsunfähig ist. Das BEM, das zur Fürsorgepflicht des Arbeitgebers für erkrankte Mitarbeiter gehört, ist nicht nur für Behinderte und Schwerbehinderte, sondern für sämtliche Beschäftigte und unabhängig von der Betriebsgröße durchzuführen. Es dient der möglichst frühzeitigen Erkennung von gesundheitlichen Problemen der Beschäftigten. Sinn und Zweck dieser Regelung ist es, umgehend zu klären, wie die Arbeitsunfähigkeit überwunden, Fehlzeiten verringert und mit welchen Hilfen und Leistungen einer erneuten Arbeitsunfähigkeit vorgebeugt werden kann. Liegen die Voraussetzungen zur Durchführung eines Eingliederungsmanagements vor, dann nimmt die Personalabteilung Kontakt mit der betroffenen Mitarbeiterin/dem betroffenen Mitarbeiter auf. Es wird ein Gespräch zum Eingliederungsmanagement angeboten und darüber aufgeklärt, dass auf Wunsch der Mitarbeiterin bzw. des Mitarbeiters auch

eine Personalratsvertreterin oder ein Personalratsvertreter (ggf. auch die Schwerbehindertenvertretung, die Frauenvertreterin und die Betriebsärztin) teilnehmen können. Wenn die/der Betroffene die Durchführung des BEM wünscht, wird dieses durchgeführt. Wenn die festgelegte Maßnahme zum Erfolg geführt hat, ist das BEM beendet. Dasselbe gilt, wenn der Betroffene unabhängig von der Verfahrensstufe dies wünscht. Das BEM ist auch dann beendet, wenn in einem weiteren Gespräch festgestellt wird, dass weitere Maßnahmen nicht möglich bzw. nicht Erfolg versprechend sind.

Die Personalabteilung hat das Verfahren zur Durchführung des BEM im Sommer 2007 mit mir im Einzelnen geregelt. Wir haben vereinbart, dass nur die Eckdaten des BEM zur Personalakte genommen werden. Diese Daten umfassen insbesondere Gesprächsangebote der Personalabteilung mit Datum, Abschluss des BEM mit Ergebnis und Datum bzw. Ablehnung der Durchführung des BEM mit Datum. Alle übrigen Unterlagen und Gesprächsinhalte werden dagegen nicht Gegenstand der Personalakte, da sie die/den Betroffene(n) nicht unmittelbar in ihrem/seinem Arbeitsverhältnis betreffen.

Entscheidet sich der/die Beschäftigte für die Durchführung des BEM, muss eine ausdrückliche Einwilligungserklärung für die Verarbeitung der in diesem Zusammenhang anfallenden personenbezogenen Daten eingeholt werden. Die Gesprächsinhalte unterliegen einer absoluten Geheimhaltungspflicht der Gesprächsteilnehmer bzw. des sog. Integrationsteams. Die Daten werden ausschließlich zur Durchführung des BEM erhoben und verarbeitet, sorgfältig aufbewahrt und 3 Jahre nach Abschluss des Verfahrens entweder qualifiziert vernichtet oder - auf Wunsch - an die /den Betroffenen herausgegeben.

Auf Anfrage habe ich der Personalabteilung bestätigt, dass der Personalrat gemäß der einschlägigen Rechtsprechung einen Anspruch auf regelmäßige Information über die langzeiterkrankten Kolleginnen und Kollegen (unabhängig von einem bereits eingeleiteten BEM) hat. Einer Zustimmung der Betroffenen zu der Datenübermittlung bedarf es nicht. Die Rechtsprechung begründet diese Pflicht damit, dass der Personalrat nur mit diesen Informationen in der Lage ist, zu überwachen, dass

der Arbeitgeber seiner Verpflichtung zur Durchführung des BEM nachkommt (§ 84 Abs. 2 S. 7 SGB IX). Aus dem gleichen Grund erhält auch die Schwerbehindertenvertretung nun 1/4jährlich eine Namensliste mit allen schwer behinderten und den Schwerbehinderten gleichgestellten Langzeiterkrankten.

## **2. Auswertungen Krankheitstage**

Im Herbst 2007 ist die HA Personal an mich mit der Bitte um eine datenschutzrechtliche Einschätzung zu den Möglichkeiten der Auswertung von Krankheitstagen herangetreten.

Dabei habe ich folgenden Rechtsstandpunkt eingenommen:

Die Auswertung von Krankheitsdaten ist zur Wahrung berechtigter Interessen des Arbeitgebers rechtlich zulässig. Der Zweck des Arbeitsverhältnisses ist der Austausch von Arbeitsleistung gegen Zahlung von Arbeitsentgelt. Von daher entspricht es einem berechtigten Interesse des Arbeitgebers festzustellen, inwieweit dieses Austauschverhältnis durch Krankheits- und Fehlzeiten gestört ist. Berechtigte Belange des Arbeitnehmers, dem **rbb** diese Erkenntnisse zu verwehren, bestehen nicht.

In diesem Zusammenhang habe ich noch einmal an den datenschutzrechtlichen Grundsatz erinnert, wonach die Mitarbeiterinnen und Mitarbeiter des **rbb** nur jeweils auf diejenigen personenbezogenen Daten Zugriff erhalten dürfen, die sie konkret für ihre Arbeit benötigen. Dieser Grundsatz gilt selbstverständlich auch die für Führungskräfte. Danach ist eine Weitergabe von Auswertungen der Krankheitsdaten nur an die jeweils zuständigen Führungskräfte zulässig. Im Übrigen kommen nur anonymisierte Auswertungen in Betracht.

### **3. Neuer Tarifvertrag für arbeitnehmerähnliche Personen des Rundfunk Berlin-Brandenburg**

Am 1. Januar 2008 ist der neue Tarifvertrag für arbeitnehmerähnliche Personen des **rbb** in Kraft getreten, mit dem die entsprechenden Tarifverträge von ORB und SFB abgelöst wurden. Geregelt sind darin Ansprüche auf Urlaubsentgelt, auf Zuschuss im Krankheitsfall zum Mutterschaftsgeld und auf Ausgleichszahlungen bei Nichteinhaltung der Ankündigungsfristen.

In diesem Zusammenhang hat mir die HA Personal die Entwürfe für die neuen Antragsformulare zur datenschutzrechtlichen Prüfung vorgelegt. Meine kleineren Änderungsvorschläge wurden umgesetzt, so dass jetzt sichergestellt ist, dass nur diejenigen personenbezogenen Daten der arbeitnehmerähnlichen Personen erhoben werden, die für die Prüfung der geltend gemachten Ansprüche zwingend erforderlich sind.

## **IV. Sonstiges**

### **1. Reuters Mediendienste**

Im August 2007 hat der **rbb** einen Vertrag mit der Nachrichtenagentur Reuters über die Zulieferung von Börsendaten via Internet abgeschlossen. In seinen AGB informiert Reuters darüber, dass mit Hilfe von entsprechenden Cookies Informationen über die Art und Weise, in der der Kunde Finanzinformationsdienste verwendet, erhoben werden. Durch die Nutzung der Finanzinformationsdienste willigt der Kunde ein, dass Reuters zum Zwecke des Supports, der Kapazitätsplanung, zur Erkennung und Vermeidung von Verstößen gegen die Netzwerksicherheit, gegen Gesetze oder vertragliche Bestimmungen und für andere Aktivitäten, die der Durchführung, Verwaltung und Verbesserung der Dienste von Reuters dienen, Nutzungsdaten speichern und verarbeiten darf.

Ich konnte den neuen Modalitäten der Zusammenarbeit mit Reuters unter folgenden Bedingungen zustimmen:

Für die Nutzung der Reuters-Finanzdienste wird ein separater PC verwendet. An diesem PC müssen sich die Mitarbeiter/innen mit ihrer jeweiligen ID und dem Passwort im **rbb**-Netz zu Beginn ihrer Arbeit an und bei Ende ihrer Arbeit wieder abmelden. Die Nutzung des Reuters-Finanzdienstes erfolgt mit einem einzigen **rbb**-account, den alle Wirtschaftsredakteure/innen nutzen. Somit ist Reuters nicht in der Lage, Einzelprofile der **rbb**-Mitarbeiterinnen und -Mitarbeiter zu erstellen. Reuters wurde kein Remote-Zugriff eingeräumt.

## 2. Löschfristen bei SAP

Personenbezogene Daten müssen gem. § 36 Abs. 1 **rbb**-Staatsvertrag i. V. m. § 17 Abs. 3 S. 1 BInDSG gelöscht werden, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Daher sind in den Dienstvereinbarungen zu den einzelnen SAP-Modulen vor einigen Jahren unter meiner Mitwirkung für sämtliche personenbezogenen Daten entsprechend der einschlägigen bereichsspezifischen gesetzlichen Regelungen (z. B. Steuer-, Sozialversicherungsgesetze, etc...) Aufbewahrungsfristen festgelegt worden.

Die Datenverarbeitung der SAP-Daten wird im Informationsverarbeitungszentrum (IVZ) für den **rbb** durchgeführt.

Anlässlich eines Treffens der Datenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten am 10. Mai 2007 beim IVZ erfuhr ich, dass bislang nur die SAP R/2-Altdateien ordnungsgemäß gelöscht und vernichtet worden sind. In SAP R/3 ist bislang keine Löschung erfolgt. Auf Nachfrage bei den Verantwortlichen im **rbb** erhielt ich dazu die Auskunft, dass im SAP-Produktivsystem das physische Löschen von Daten „aus Ordnungsmäßigkeitsgründen nicht vorgesehen“ sei. Gemeinsam mit dem IVZ werde man nach einer Lösung suchen. Inzwischen habe ich erfahren, dass mit dem Release-Wechsel nach ERP 6.0 Ende Juni 2008 ein Report zum Löschen

personenbezogener Daten zur Verfügung stehen wird. Nach dem Release-Wechsel beabsichtige ich eine Kontrolle der Umsetzung des vereinbarten Konzepts zu den Aufbewahrungsfristen.

### **3. Webcam der streamcast media GmbH auf dem Alexanderplatz**

Die Tochtergesellschaft des **rbb**, streamcast media GmbH, hat im Sommer 2007 auf dem Park Inn-Hotel am Alexanderplatz eine Webcam angebracht. Das übertragene Bild der Kamera ist als Livestream auf der von der streamcast media GmbH betriebenen Homepage zu sehen. Im Vorfeld war ich um eine datenschutzrechtliche Einschätzung gebeten worden.

Da die streamcast media GmbH eine juristische Person des Privatrechts ist, hat sie das Bundesdatenschutzgesetz (BDSG), hier insbesondere § 6 b BDSG, zu beachten. Diese Vorschrift lässt die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur unter engen Voraussetzungen zu, die hier allesamt nicht einschlägig gewesen wären.

Die Webcam stellt eine optisch-elektronische Einrichtung i. S. d. § 6 b BDSG dar und der Alexanderplatz ist ein öffentlich zugänglicher Raum, weil darunter auch umgrenzte Plätze gefasst werden. Es kam also entscheidend darauf an, ob eine Beobachtung i. S. dieser Vorschrift geplant war. Eine Beobachtung ist dann ausgeschlossen, wenn mithilfe der übertragenen Bilder überhaupt keine Personen erkannt werden können. In diesem Fall fallen gar keine personenbezogenen Daten an.

Ich habe der streamcast media empfohlen, die Zoomstufen der Kamera so einzustellen, dass keine Personen erkennbar sind, und dafür Sorge zu tragen, dass die Webcam nicht unbefugt zur Videoüberwachung i. S. d. § 6 b BDSG umfunktioniert wird.

#### **4. Diverse Einzelvorgänge**

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

Eine Kollegin der Marketing-Abteilung habe ich zur datenschutzrechtlich korrekten Gestaltung einer Anmeldekarte für die von der Radiowelle Antenne Brandenburg durchgeführten Tour de Priegnitz beraten. Es ging darum, durch einen entsprechenden Hinweis auf dem Formular klarzustellen, dass die Einwilligung in die Benutzung der persönlichen Daten durch die Kooperationspartner des **rbb** zu Werbezwecken freiwillig und keine Voraussetzung für die Teilnahme an der Tour ist.

Ein Kollege wandte sich an mich mit der Frage, ob die Einrichtung eines gemeinsamen Laufwerks für eine ganze Abteilung datenschutzrechtlich zulässig sei. Ich habe ihm erklärt, dass dies dann der Fall sei, wenn dort Daten abgelegt würden, deren Kenntnis für sämtliche Mitarbeiter der Abteilung erforderlich seien. Ansonsten müsse es spezielle Laufwerke für die einzelnen Bereiche innerhalb der Abteilung geben - jedenfalls, wenn dort (auch) personenbezogene Daten abgelegt werden.

#### **V. Informationsmaßnahmen**

Meine Informations- und Schulungsaufgabe habe ich im Berichtszeitraum wahrgenommen, indem ich in verschiedenen hausinternen Besprechungen auf aktuelle und für den jeweiligen Aufgabenbereich relevante Fragen des Datenschutzes eingegangen bin. Außerdem habe ich eine datenschutzrechtliche Schulung für die Rundfunkgebührenbeauftragten und eine weitere für die Auszubildenden des **rbb** durchgeführt.

##### **1. Datenschutzrechtliche Schulung der Rundfunkgebührenbeauftragten**

Am 10. Juli 2007 habe ich zusammen mit dem Systemverantwortlichen für IT-Sicherheit, Herrn Gerry Wolff, eine datenschutzrechtliche Schulung der Rundfunk-

gebührenbeauftragten durchgeführt. Dabei wurden neben allgemeinen Fragen zu Datenschutz und Datensicherheit insbesondere auch Fragen zum Einsatz elektronischer Datenverarbeitungsgeräte erörtert. Von mehreren Rundfunkgebührenbeauftragten wurde der Wunsch nach dem Einsatz von mobilen Datenverarbeitungsgeräten wie Laptops, Blackberries u. ä. geäußert. Bislang ist der Einsatz von mobilen Geräten für die Rundfunkgebührenbeauftragten aus Datensicherheitsgründen beim **rbb** untersagt. Es wurde verabredet, zum Thema „Einsatz von mobilen Geräten“ im Oktober 2007 eine Sondersitzung durchzuführen. Bis dahin sollte der konkrete Bedarf gründlich analysiert werden. Im Berichtszeitraum hat keine weitere Sitzung stattgefunden. Der Leiter der Abteilung Rundfunkgebühren ist in dieser Angelegenheit bislang nicht wieder an mich herangetreten.

## **2. Datenschutzrechtliche Schulung der Auszubildenden**

Am 3. August 2007 habe ich zusammen mit dem Kollegen aus der Abteilung Informations- und Kommunikationstechnik, Herrn Ralf Fleischhauer, ein zweistündiges Einführungsseminar zum Thema „Datenschutz und Datensicherheit im **rbb**“ für unsere neuen Auszubildenden durchgeführt. Mithilfe eines anschaulichen Videofilms wurden die neuen Kolleginnen und Kollegen zunächst für die Themen Datenschutz und Datensicherheit sensibilisiert. Sodann habe ich die datenschutzrechtliche Situation dargestellt und die für den **rbb** einschlägigen Rechtsnormen im Einzelnen vorgestellt. Anschließend habe ich die konkreten Anforderungen an den Umgang mit personenbezogenen Daten beim **rbb** im Einzelnen erläutert. Herr Fleischhauer hat meine Ausführungen zu den technischen Anforderungen mit praktischen Demonstrationen am PC ergänzt.

## **D. Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung**

### **I. Allgemeines**

Für die Einziehung der Rundfunkgebühren ist seit 1976 die Gebühreneinzugszentrale (GEZ) in Köln zuständig. Dort wurden zum 31. Dezember 2007 die Daten von rund 39,7 Mio. aktiven Teilnehmerkonten verarbeitet. Damit sind insgesamt rund

38,9 Mio. Hörfunkgeräte, 32,9 Fernsehgeräte und ca. 120.000 neuartige Empfangsgeräte gebührenpflichtig; gebührenbefreit sind 3,6 Mio. Hörfunkgeräte, 3,3 Mio. Fernsehgeräte und ca. 2.000 neuartige Empfangsgeräte.

Bezogen auf den **rbb** ergeben sich zum 31. Dezember 2007 folgende Zahlen: 2,58 Mio. gebührenpflichtige und 0,38 Mio. gebührenbefreite Hörfunkgeräte, 2,30 Mio. gebührenpflichtige und 0,38 Mio. gebührenbefreite Fernsehgeräte sowie ca. 4.000 gebührenpflichtige und keine befreiten neuartigen Empfangsgeräte.

Für den Datenschutz der Rundfunkteilnehmer/innen gelten in erster Linie die bereichsspezifischen Regelungen des Rundfunkgebührenstaatsvertrages und - für die Teilnehmerinnen und Teilnehmer in Berlin und Brandenburg - gemäß § 35 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 RGebStV).

## II. Anfragen und Auskunftersuchen

Anfragen und Auskunftersuchen im Hinblick auf Rundfunkteilnehmerdaten im Bereich des **rbb** gehen sowohl bei der GEZ und dem **rbb** als auch bei den zuständigen Landesdatenschutzbeauftragten von Berlin und Brandenburg ein. Anfragen aus dem Bereich der Rundfunkteilnehmerdatenverarbeitung leiten die Landesdatenschutzbeauftragten mir jeweils mit der Bitte um Stellungnahme zu.

Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten der betrieblichen 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 2007 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	08
Fragen bzgl. der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung	12
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen	26
Verlangen, Teilnehmerdaten nicht zu anderen Zwecken zu nutzen bzw. zu übermitteln	0
Anfragen von Finanzämtern nach Daten (insbes. Bankverbindungen) von Rundfunkteilnehmern	03
Anfragen von Kommunalkassen o. sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Rundfunkteilnehmern	06
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz	11
<b>Anzahl Vorgänge insgesamt</b>	<b>66</b>

Ich selbst habe in 2007 folgende Vorgänge bearbeitet:

Bitte um Kontenklärung mit entsprechender Aufstellung der Zahlungseingänge	02
Fragen im Zusammenhang mit der Glaubhaftmachung der Befreiungsvoraussetzungen	04
Auskunftersuchen über die zur eigenen Person gespeicherten Daten	05
<b>Anzahl Vorgänge insgesamt:</b>	<b>11</b>

Im Vergleich zum Vorjahr (insgesamt 86 Anfragen aus dem Sendegebiet des **rbb**) ist also eine leicht rückläufige Tendenz zu verzeichnen.

### **III. np-Datenbank**

Schon in meinen beiden vorhergehenden Tätigkeitsberichten hatte ich über die Pläne der GEZ zur Einrichtung einer np (= Nichtprivaten)-Datenbank zur zielgerichteten Bearbeitung und Ausschöpfung des nichtprivaten Marktes berichtet. Im Vorfeld hatte die GEZ Pläne entwickelt, die nach mehrheitlicher Auffassung im AK DSB nicht datenschutzrechtskonform waren. Nach intensiven Diskussionen hat die GEZ dem AK DSB zu seiner Sitzung am 21./22. September 2006 ein überarbeitetes Konzept vorgelegt, gegen das keine datenschutzrechtlichen Einwände mehr bestanden. Nach einer anschließenden erneuten Überarbeitung des Konzeptes durch die GEZ in Zusammenarbeit mit den Rundfunkgebührenabteilungen der einzelnen Häuser wurden dann allerdings weitere Fragen und Probleme aufgeworfen.

In der Folgezeit haben erneut diverse Gespräche zur Klärung dieser Fragen zwischen Vertretern der GEZ, den Rundfunkgebührenabteilungen und den Rundfunkdatenschutzbeauftragten stattgefunden. In dem nunmehr gemeinsam verabschiedeten aktuellen Konzept ist sichergestellt, dass grundsätzlich alle personenbezogenen Daten von Firmen, die nicht als Rundfunkteilnehmer identifiziert werden konnten - wie in § 8 Abs. 4 RGebStV vorgeschrieben und wie auch für die potentiellen privaten Rundfunkteilnehmer praktiziert -, maximal 12 Monate gespeichert werden. Das System ist inzwischen produktiv.

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

Am 7. und 8. Februar 2008 fand erneut eine datenschutzrechtliche Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Hessen, Brandenburg und Berlin statt. Prüfungsinhalte waren im Wesentlichen die Datenübermittlung der GEZ an Dritte, das Zugriffskonzept in DV 2005 und im Verfahren BDONAB, die Möglichkeiten und die Bedingungen für Telearbeit, die Organisation im Befreiungsverfahren sowie das Löschkonzept. Weitere Schwerpunkte der Prüfung waren die Besichtigung eines Sachbearbeiterplatzes und der Workflow bei der Befreiung von der Rundfunkgebührenpflicht. An der Prüfung waren neben verschiedenen Vertretern der GEZ und Leitern der Rundfunkgebührenabteilungen der von der Prüfung unmit-

telbar betroffenen Rundfunkanstalten als Auskunftspersonen auch einige Rundfunkdatenschutzbeauftragten - u. a. ich selbst - anwesend.

Ein Ergebnis der Prüfung liegt noch nicht vor.

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

### **I. Allgemeines**

Das Informationsverarbeitungszentrum (IVZ) ist das gemeinsame Rechenzentrum von MDR, **rbb**, Radio Bremen, NDR, SR und DLR mit Sitz in Potsdam. Für die datenschutzrechtliche Kontrolle sind alle Datenschutzbeauftragten der Betreiber-Anstalten gemeinsam zuständig. Federführend wird die Arbeit von mir als Datenschutzbeauftragte der ortsansässigen Rundfunkanstalt durchgeführt.

In Grundsatzangelegenheiten beziehe ich die Kolleginnen und Kollegen der anderen Rundfunkanstalten ein. Regelmäßig (durchschnittlich einmal pro Jahr) finden Sitzungen aller beteiligten Rundfunkdatenschutzbeauftragten beim IVZ statt, auf denen uns der Geschäftsführer, Herr Dr. Greten, und seine Mitarbeiter/innen über die neuesten Entwicklungen mit datenschutzrechtlicher Relevanz informieren.

### **II. Spezielles**

Im Berichtszeitraum fand am 10. Mai 2007 eine Besprechung der Rundfunkdatenschutzbeauftragten mit Herrn Dr. Greten und seinen Mitarbeitern beim IVZ statt.

#### **1. Neue Hörfunkdatenbank**

Herr Dr. Greten, informierte uns über die geplante neue Hörfunkdatenbank. Die erste Komponente (Schallplattenkatalog) ist bereits Mitte 2007 in den produktiven Betrieb überführt worden. Dieser Teil wurde für alle Kooperationspartner im IVZ-Rechenzentrum durchgeführt. Für die Umsetzung der Löschfristen bezüglich der

User-Daten kommt ein Administratorentool analog zu FESAD zum Einsatz. Ein spezifisches Löschen von User-Daten für eine einzelne Rundfunkanstalt ist nicht möglich. Die User-Daten werden entsprechend der Löschkriterien für alle Rundfunkanstalten einheitlich gelöscht. Spezifische Logdaten (z. B. welcher User eine Recherche veranlasst hat), können laut IVZ nicht abgefragt werden.

## **2. Kein Einsatz des SAP-Solution Managers**

In einer Kurzpräsentation wurde uns das zentrale Monitoringtool der SAP „Solution Manager“ vorgestellt. Dabei wurde deutlich, dass aufgrund der darin bereitgestellten erweiterten Funktionalitäten der Einsatz des Tools eine strategische Neuausrichtung beim IVZ erfordert hätte. Wegen des hierarchischen Aufbaus im Change Management, hätten die Endanwender indirekt Zugriff auf Systeme anderer Rundfunkanstalten erhalten. Die Vergabe der Berechtigungen hätte nicht mehr in der Hoheit der Rundfunkanstalt verbleiben können. Eine Lösung hätte in dem Einsatz von dezentralen Solution Managern bestanden. Nur auf diese Weise hätte die Forderung nach der strikten Trennung der Mandanten-Netze aufrechterhalten werden können. Die Folge wären allerdings zusätzliche Kosten und Administrationsaufwand gewesen. Die Datenschutzbeauftragten hatten Herrn Dr. Greten gebeten, diesen Sachverhalt im Lenkungsausschuss zur Klärung zu bringen. *(Anmerkung: Inzwischen hat sich das IVZ gegen den Einsatz des Solution Managers entschieden.)*

## **3. Neues von den Teleheimarbeitsplätzen**

Wie berichtet, nutzen seit 2006 vier Mitarbeiter im Bereich der SAP-Anwendungsentwicklung an zwei Arbeitstagen pro Woche einen Teleheimarbeitsplatz. In einer Zusatzvereinbarung zum Arbeitsvertrag sind mit den Mitarbeitern umfangreiche Regelungen zu Datenschutz und Datensicherheit getroffen worden. Auf der Sitzung am 10. Mai 2007 wurde beantragt, zukünftig den Zugriff auch auf die produktiven Mandaten der Rundfunkanstalten zu gewähren. Da uns die Erforderlichkeit dafür nicht plausibel dargelegt werden konnte, haben wir empfohlen, die gegenwärtige Verfahrensweise beizubehalten. Im Falle eines entsprechenden Er-

fordernisses sollte die Zustimmung der Datenschutzbeauftragten erneut eingeholt werden.

Ein weiteres Thema auf der Sitzung am 10. Mai 2007 war die Überprüfung der externen Firmenzugänge auf das interne Datennetz des IVZ auf Sicherheit und Notwendigkeit. Die externen Firmenzugänge waren auf Anforderung der Rundfunkanstalten mit ständiger Einwahlmöglichkeit konfiguriert worden. Die Datenschutzbeauftragten haben empfohlen, dies zu ändern und die Zugänge nur temporär zu öffnen. Herr Dr. Greten hat eine Behandlung des Themas im Lenkungsausschuss zugesagt.

#### **4. BSI-Zertifizierung**

Am 7. März 2008 ist das IVZ (Rechenzentrum) vom Bundesamt für Sicherheit in der Informationstechnik mit dem IT-Sicherheitszertifikat nach ISO2 7001 Zertifikat auf der Basis von IT-Grundschutz zertifiziert worden. Das Zertifikat ist zwei Jahre gültig.

Im Oktober 2007 hatte das IVZ einen entsprechenden Antrag eingereicht. In deren Folge hat ein Audit-Team das IVZ Rechenzentrum geprüft. Per Losentscheid wurde ein repräsentativer Pflichtbaustein ausgelost, der dann genauer untersucht wurde. Im Ergebnis der Überprüfung wurde ein Audit-Report erstellt. Nach Abschluss geringfügiger Nacharbeiten wurde das Zertifikat überstellt. Mit dieser Zertifizierung ist die Weichenstellung für eine datensicherheitsgerechte Verwaltung der Daten nach außen dokumentiert.

Die Rundfunkdatenschutzbeauftragten haben sich für eine Re-Zertifizierung in 2010 ausgesprochen.

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

Das ARD-Infocenter hat im Sommer 2007 eine computergestützte Erfassungssoftware installiert, mit der die direkten und indirekten Kontakte (Besucher, Anfragen per Mail und Telefon u. ä.) regelmäßig erfasst werden. Die externen Kontakte werden anonym in der Datenbank gespeichert. Ausgewertet werden ausschließlich z. B. Anzahl der Besucher, Zeitpunkt des Besuchs, gestellte Frage etc... Ich habe mich davon überzeugt, dass anhand des neuen Systems keine personalisierten Rückschlüsse auf das Personal des ARD-Infocenters möglich sind und habe daher keine Einwände gegen das System erhoben.

Zum 1. Oktober 2007 sind die Dienstanweisung zur Verarbeitung personenbezogener Daten im ARD- Hauptstadtstudio, die Dienstanweisung für die Nutzung von Internet und E-Mail und die Dienstanweisung für die Nutzung von Exchange über Outlook (OWA/OMA) im ARD Hauptstadtstudio in Kraft getreten. Alle drei Dienstanweisungen sind in Abstimmung mit mir zustande gekommen und lehnen sich eng an die entsprechenden Regelwerke im **rbb** an.

## **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 wechselt alle zwei Jahre. Gegenwärtig hat der Datenschutzbeauftragte des NDR, Herr Maximilian Merten, den Vorsitz. Herr Gardemann von der Deutschen Welle ist sein Stellvertreter.

Im Berichtszeitraum fanden zwei reguläre Sitzungen des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) statt.

Am 26./27. April 2007 hat die Arbeitsgruppe beim ZDF in Mainz getagt. U.a. haben wir uns mit datenschutzrechtlichen Aspekten der Neugestaltung der Rundfunkfi-

nanzierung beschäftigt. Ferner stand die ursprünglich geplante Grundverschlüsselung bei ASTRA auf der Agenda. Der Arbeitskreis hat in diesem Zusammenhang seinen Standpunkt bekräftigt, wonach auch zukünftig die Möglichkeit zum anonymen Rundfunkempfang gewährleistet bleiben muss. Inzwischen wird die Grundverschlüsselung bei Astra nicht mehr angestrebt. Weitere Themen der Sitzung waren u. a. das betriebliche Eingliederungsmanagement nach § 84 Abs. 2 SGB IX sowie datenschutzrechtliche Fragen im Zusammenhang mit der Datenerhebung und -übermittlung zu Gehalts- und Urlaubsansprüchen freier Mitarbeiter.

Am 22./23. November 2007 haben wir beim Hessischen Rundfunk in Frankfurt getagt. Auf dieser Sitzung wurden hauptsächlich Themen des Rundfunkteilnehmerdatenschutzes, wie z. B. Änderungen im Zugangssystem für die Rundfunkgebührenbeauftragten auf die GEZ-Datenbank (BDONAB), die konkrete Ausgestaltung der geplanten np-Datenbank, das Verfahren zur Befreiung von der Rundfunkgebührenpflicht sowie das Online-Anmeldeverfahren der GEZ über Formulare im Internet besprochen. Herr Merten wurde mit Wirkung ab 1. Januar 2008 für die Dauer von zwei Jahren zum Vorsitzenden und Herr Gardemann zu seinem Stellvertreter gewählt.

## **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. Für die damit zusammenhängenden datenschutzrechtlichen Fragestellungen verrete ich den AK DSB als ständiges beratendes Mitglied in dem IT-Sicherheitsgremium.

Im Berichtszeitraum hat das Gremium dreimal getagt: am 9. Mai 2007 beim Deutschlandradio in Berlin, am 12. September 2007 bei der Deutschen Welle in Bonn und am 16. Januar 2008 beim **rbb** in Berlin. U. a. hat das Gremium die Mindeststandards für die IT-Sicherheit mobiler Produktionsnetzwerke verabschiedet, sich für ein einheitliches IT-Sicherheitsinformationssystem ausgesprochen, die Ergebnisse des IT-Sicherheits-Audits des TÜV Rheinland vom 20. Februar 2008 ausgewertet und ein Konzept für die Behandlung von IT-Sicherheitsvorfällen im ARD-

CN erarbeitet. Außerdem hat sich das Gremium auf die Bitte des AK DSB ausführlich mit der Frage der Notwendigkeit der Speicherung von IP-Adressen zur Gewährleistung der Datensicherheit des Online-Angebotes der Rundfunkanstalten befasst.

### **III. Arbeitskreis Medien der Staatlichen Datenschutzbeauftragten**

Im Arbeitskreis Medien diskutieren die Datenschutzbeauftragten von Bund und Ländern unter dem Vorsitz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Frau Dagmar Hartge, aktuelle und strategische Fragen des Datenschutzes aus den Bereichen Telekommunikations-, Multimedia- und Rundfunkrecht. An einem Teil der Sitzungen des Arbeitskreises nimmt regelmäßig ein Vertreter des AK DSB (in der Regel der Vorsitzende) teil.

Am 19. Februar 2008 habe ich den Vorsitzenden des AK DSB, Herrn Merten, auf der Sitzung des AK Medien vertreten. Themen waren der Einsatz von Spam-Filtern und Virensclannern in der Brandenburgischen Landesverwaltung, der Stand der rundfunkrechtlichen Änderungsstaatsverträge, das Verfahren zur Befreiung von der Rundfunkgebührenpflicht und die Vorratsdatenspeicherung in der elektronischen Kommunikation sowie Datenschutz im Web 2.0.

### **IV. Gespräch mit Vertretern des LDSB Brandenburg und des BerIDSB**

Zwischen den zuständigen Sachbearbeitern der Brandenburgischen Landesdatenschutzbeauftragten (LDSB Brandenburg), des Berliner Datenschutzbeauftragten (BerIDSB) und mir findet auf der Arbeitsebene regelmäßig ein Gedankenaustausch zu datenschutzrechtlichen Fragestellungen im Bereich der Rundfunkteilnehmerdatenverarbeitung statt.

Am 1. Juni 2007 habe ich zusammen mit dem Systemverantwortlichen IT-Sicherheit, Herrn Wolff, dem Leiter der Abt. Rundfunkgebühren, Herrn Schermuck, und meinem für Fragen des Rundfunkgebührenrechts zuständigen Kollegen im Justizariat, Herrn Witte, ein Gespräch mit den Herren Hermerschmidt (LDSB Brandenburg) und Dr. von Petersdorff (BerIDSB) geführt. Themen waren u. a. das Verfahren

bei der Befreiung von der Rundfunkgebühr (insbesondere Anerkennung von Drittbescheinigungen der Sozialleistungsträger durch die GEZ), eine geplante Prüfung der Rundfunkgebührenbeauftragten (*Anm.: hat bislang nicht stattgefunden*), Zugriffsmöglichkeiten der Rundfunkgebührenbeauftragten auf das Rundfunkteilnehmerdatenverarbeitungssystem der GEZ, die geplante np-Datenbank und der Sachstand der geplanten Rundfunkänderungsstaatsverträge.

## **V. Teilnahme an Veranstaltungen**

### **1. Internationales Symposium zum Thema „Datenschutz beim digitalen Fernsehen“**

Am 3. September 2007 habe ich an dem internationalen Symposium zum Thema „Datenschutz beim digitalen Fernsehen“ im Internationalen Congress Centrum Berlin (ICC) teilgenommen. Veranstalter war der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Dabei wurden insbesondere Fragen im Zusammenhang mit der geplanten Verschlüsselung von Rundfunkprogrammen erörtert. Die Teilnehmerinnen und Teilnehmer des Symposiums waren sich darüber einig, dass es unterschiedliche Lösungen für unterschiedliche Angebote geben müsse. Bei einem Fernsehvollprogramm besteht kein bzw. nur ein geringer Bedarf zur Verarbeitung von personenbezogenen Daten der Nutzer. Anders ist die Situation z. B. bei Pay-TV oder Teleshopping zu beurteilen.

### **2. 2. Europäischer Datenschutztag**

Am 28. Januar 2008, dem 2. Europäischen Datenschutztag, fand in der Robert-Jungk-Oberschule in Berlin/Wilmersdorf eine gemeinsame Veranstaltung des Berliner Beauftragten für Datenschutz und Informationsfreiheit und des Bundesbeauftragten für den Datenschutz und Informationsfreiheit statt. Unter der Überschrift „Datenschutz 2. 0 - Web 2. 0“ wurde über die besonderen datenschutzrechtlichen Risiken, die das Web 2. 0 für die Nutzer in sich birgt, diskutiert. Ich habe an der Veranstaltung zusammen mit dem Systemverantwortlichen für IT-Sicherheit, Herrn

Wolff, teilgenommen. Wir konnten viele Anregung für die datenschutzgerechte Ausgestaltung der neuen Plattform „myFritz“ des **rbb** mitnehmen.

Berlin, 20. Juni 2008

gez. Anke Naujock