6. Tätigkeitsbericht

der Beauftragten für den Datenschutz
des Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2008 bis 31. März 2009

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

Inhaltsverzeichnis

Vorbemerkung

Im vergangenen Jahr hat das Thema Datenschutz u. a. aufgrund der intensiven Berichterstattung über die Mitarbeiterüberwachung durch verschiedene Supermarkt- und Discounterbetreiber, die Deutsche Telekom und die Deutsche Bahn AG in der öffentlichen Wahrnehmung erheblich an Bedeutung gewonnen.

Dass vergleichbare Spitzelmethoden beim Rundfunk Berlin-Brandenburg stattfinden könnten, halte ich für ausgeschlossen. In diesem Zusammenhang ist das engmaschige Netz an einschlägigen Regelungen hervorzuheben: neben dem Berliner Datenschutzgesetz und den bereichsspezifischen Datenschutznormen existieren beim **rbb** zahlreiche Dienstvereinbarungen und Richtlinien zum Thema Arbeitnehmerdatenschutz. Danach ist z. B. das Abhören von Telefongesprächen generell verboten. Die Auswertung von Telefonverbindungen und Protokolldaten im Zusammenhang mit der Nutzung von Internet- und E-Mail ist lediglich in begründeten Verdachtsfällen und unter Einhaltung eines genau definierten Verfahrens gestattet (s. dazu S. 20 f.). Dies allein bietet selbstverständlich keine Sicherheit. Entscheidend ist die Umsetzung der Regelungen. Aber auch diesbezüglich habe ich ein gutes Gefühl: In der täglichen Praxis zeigt sich, dass bei den Führungskräften, den Fachverantwortlichen und vor allem auch bei den Administratoren, die ja zumindest theoretisch über sehr weitreichende technische Datenauswertungsmöglichkeiten verfügen, eine hohe Sensibilität für die Themen Datenschutz und Datensicherheit vorhanden ist. Nicht zuletzt trägt auch das große Engagement des Personalrats auf diesem Gebiet dazu bei, dass Datenschutz und Datensicherheit im **rbb** groß geschrieben werden.

Neben dem Arbeitnehmerdatenschutz bildete auch der Datenschutz beim Rundfunkgebühreneinzug wieder einen Schwerpunkt meiner Arbeit.

Auch im vergangenen Jahr gab es für mich keinen Anlass, eine förmliche Beanstandung auszusprechen.

Bei dem stellvertretenden behördlichen Datenschutzbeauftragten, Herrn Dr. Bismark, und dem Systemverantwortlichen für IT-Sicherheit, Herrn Gerry Wolff, bedanke ich mich für ihre Unterstützung.

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

I. Gesetzliche Grundlagen

Die Rechtsgrundlagen für die Datenschutzbeauftragte 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).

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).

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

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.

Mit Wirkung zum 01. Januar 2009 hat die Intendantin den Leiter der Revision, Herrn Dr. Bismark, zum stellvertretenden behördlichen Datenschutzbeauftragten ernannt. In Anlehnung an meine eigene ist seine Amtszeit bis zum 30. Juni 2011 befristet. Für die Datensicherheit im **rbb** ist seit einigen Jahren der Systemverantwortliche für IT-Sicherheit, Herr Gerry Wolff, verantwortlich.

Die datenschutzrechtliche Kontrolle durch den Berliner Landesdatenschutzbeauftragten in Abstimmung mit der Brandenburgischen Datenschutzbeauftragten gemäß § 38 Abs. 8 **rbb**-Staatsvertrag beschränkte sich auch im Berichtszeitraum wieder auf die Einhaltung des Datenschutzes beim Rundfunkgebühreneinzug.

B. Entwicklung des Datenschutzrechts

I. Europa

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

In meinen früheren Berichten hatte ich bereits über das Vertragsverletzungsverfahren gegen Deutschland um die Einrichtung unabhängiger Datenschutzstellen vor dem EuGH berichtet. Die Kommission ist der Auffassung, dass bei den Länderbehörden, denen die Datenschutzaufsicht über private Stellen obliegt, die in Art. 28 Abs. 1 der Datenschutzrichtlinie (95/46/EG) geforderte „völlige Unabhängigkeit" nicht gegeben sei. Inzwischen hat sich der Europäische Datenschutzbeauftragte in den Rechtsstreit eingeschaltet; im Oktober 2008 wurde er vom EuGH als Streithelfer zugelassen. Das Verfahren dauert noch an.

II. Bund

1. Gesetzgebung

a) Novellierung des BKA-Gesetzes

Am 01. Januar 2009 ist die Novellierung des BKA-Gesetzes in Kraft getreten. Sie räumt den Beamten des Bundeskriminalamtes zur Terrorabwehr weitreichende Befugnisse - u. a. in § 20 k das Recht zur Online-Durchsuchung - ein. Die Neufassung des BKA-Gesetzes wurde vom Deutschen Bundestag am 12. November 2008 mit der Mehrheit der Stimmen von CDU/CSU und SPD verabschiedet. Für das zustimmungspflichtige Gesetz fand sich jedoch im Bundesrat am 28. November 2008 keine Mehrheit. Nachdem das Gesetz den Vermittlungsausschuss nach

einigen Änderungen passierte, hat der Bundesrat den geänderten Entwurf am 19. Dezember 2008 akzeptiert.

In ihrer Stellungnahme zu dem Gesetzesentwurf hatten die Medienverbände – darunter auch ARD und ZDF – vor unverhältnismäßigen Befugnissen der Ermittlungsbehörden und vor einer Aushöhlung des Zeugnisverweigerungsrechts für Journalisten und andere Berufsgeheimnisträger gewarnt. Hat die nach dem Gesetz vorgesehene einfache Verhältnismäßigkeitsprüfung ein positives Ergebnis, kann das BKA nun Telefongespräche abhören, E-Mail-Verkehr aufzeichnen und auf Kommunikationsdaten der letzten Monate zugreifen. Schon durch die Vorratsdatenspeicherung werden potentielle Informanten abgeschreckt, sich mit vertraulichen Informationen an Journalisten zu wenden. Dieser Effekt wird durch das BKA-Gesetz nochmals verschärft.

Gegen das Gesetz haben verschiedene Beschwerdeführer inzwischen Verfassungsbeschwerde erhoben.

b) Gesetz zur Durchsetzung der Rechte des geistigen Eigentums

Am 01. September 2008 ist das Gesetz zur Durchsetzung der Rechte des geistigen Eigentums in Kraft getreten. Hier stehen insbesondere die Auskunftsansprüche von Privaten gegenüber Internet-Providern wegen Urheberrechtsverletzungen im Blickpunkt der Öffentlichkeit. Unklar im Rahmen des Auskunftsanspruchs ist vor allem die Voraussetzung der „Rechtsverletzung in gewerblichem Ausmaß". Dieses kann sich sowohl aus der Anzahl der Rechtsverletzungen als auch aus der Schwere der Rechtsverletzung ergeben. Wenn ein gewerbliches Ausmaß vorliegt, eine Auskunft aber nur unter Verwendung von Verkehrsdaten erteilt werden kann, muss nach § 101 Abs. 9 UrhG eine richterliche Anordnung eingeholt werden. Die sog. Vorratsdaten i.S.v. § 113 a Telekommunikationsgesetz (TKG) dürfen für die Erteilung solcher Auskünfte nicht genutzt werden.

2. Rechtsprechung

a) Weitere Eilentscheidung des BVerfG zur Vorratsdatenspeicherung

Am 09. November 2007 hat der Deutsche Bundestag bekanntlich das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG verabschiedet. Das Gesetz war zum 01. Januar 2008 in Kraft getreten, bezogen auf die Internet-Daten erst zum 01. Januar 2009. Das Bundesverfassungsgericht (BVerfG) hat bereits mit Beschluss vom 11. März 2008 einem Eilantrag gegen die Regelungen zur so genannten Vorratsdatenspeicherung in den neu geschaffenen §§ 113 a, 113b TKG teilweise stattgegeben. Diese einstweilige Anordnung, wiederholt durch Beschluss vom 01. September 2008, wurde mit Beschluss vom 28. Oktober 2008 noch erweitert. Während bislang ein Anlass zur Erstreckung der einstweiligen Anordnung auf § 113 b S. 1 Nr. 2 und 3 TKG nicht bestand, weil weder im Bereich der Gefahrenabwehr noch des Verfassungsschutzes und der Nachrichtendienste Rechtsgrundlagen für einen Abruf der nach § 113 a TKG gespeicherten Vorratsdaten vorhanden waren, haben Bayern und Thüringen mittlerweile entsprechende Gesetze geschaffen. Das BVerfG hat deshalb die einstweilige Anordnung dahingehend erweitert, dass die nach § 113 a TKG auf Vorrat gespeicherten Daten für die Gefahrenabwehr (§ 113 b S. 1 Nr. 2 TKG) von den Telekommunikationsdiensteanbietern nur unter einschränkenden Bedingungen an die ersuchende Behörde übermittelt werden dürfen. Eine Übermittlung ist nur zulässig, wenn – zusätzlich zu den Voraussetzungen der Abrufnorm – der Abruf der Daten zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr erforderlich ist. Die übermittelten Daten dürfen nur zu den Zwecken verwendet werden, zu denen sie abgerufen wurden. Zur Strafverfolgung dürfen sie nur weitergeleitet oder verwendet werden, wenn Gegenstand der Strafverfolgungsmaßnahme eine Katalogtat i. S. von § 100 a II Strafprozessordnung (StPO) ist und die Voraussetzungen des § 100 a Abs. 1 StPO vorliegen. Für Aufgaben des Verfassungsschutzes (§ 113 b S. 1 Nr. 3 TKG) gilt,

dass im Falle eines Abrufs die Daten nur dann an die ersuchende Behörde übermittelt werden dürfen, wenn neben den Voraussetzungen der Abrufnorm auch die Voraussetzungen von §§ 1 Abs. 1, 3 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10-Gesetz) vorliegen.

Die Entscheidung des BVerfG wird zum Teil damit kritisiert, dass die betroffenen TK-Unternehmen, welche weiterhin die Kosten für die technischen Maßnahmen zur Umsetzung der Datenspeicherung gemäß § 100 Abs. 1 Nr. 1 TKG tragen müssen, benachteiligt werden. Das VG Berlin hat entschieden, dass die Kostentragungspflicht gegen die Berufsfreiheit verstößt. Es hat die Verpflichtung eines Telekommunikationsbetreibers zur Einrichtung von Vorkehrungen zur Vorratsdatenspeicherung vorläufig ausgesetzt. Diese Eilentscheidung ist nicht rechtskräftig.

Über die Nichtigkeitsklage Irlands gegen die Richtlinie vor dem EuGH hat dieser am 10. Februar 2009 mit dem Ergebnis entschieden, dass die Richtlinie auf einer zulässigen Rechtsgrundlage beruht. Danach ist die Richtlinie zu Recht auf der Grundlage des EG-Vertrages erlassen worden, da sie in überwiegendem Maß das Funktionieren des Binnenmarkts betrifft.

Arbeitgeber sind nach ganz herrschender Meinung auch dann nicht zur Vorratsdatenspeicherung verpflichtet, wenn sie – wie der **rbb** – ihren Mitarbeitern gestatten, die betrieblichen Kommunikationsmittel Telefon, E-Mail-Systeme, Internet und Intranet auch für private Zwecke zu benutzen. Der Grund liegt darin, dass sie keine öffentlich zugänglichen Telekommunikationsdienste für Endnutzer i.S.v. § 113a TKG anbieten.

b) Eilentscheidung des BVerfG zur Telekommunikationsüberwachung

In einer Eilentscheidung vom 15. Oktober 2008 hat das Bundesverfassungsgericht die Aussetzung des neu gefassten § 100 a Abs. 2, Abs. 4 StPO, der die Überwachung der Telekommunikation betrifft, abgelehnt. Gleiches gilt für die in § 160 a StPO enthaltene Regelung über den Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger, die den Antragstellern nicht weit genug ging. Die bei einer Eilentscheidung gebotene

Abwägung fiel gegen die Antragsteller aus. Die vorläufige Aussetzung des § 100 a Abs. 2 StPO könne nach Auffassung des BVerfG die Aufklärung von Straftaten erschweren. Das öffentliche Interesse an einer wirksamen Strafverfolgung überwiege.

c) Beschluss des Bundesarbeitsgerichts vom 26. August 2008 zur Videoüberwachung

Gegenstand des Verfahrens war die Entscheidung einer Einigungsstelle zur Einführung einer Videoüberwachung in einem Briefverteilzentrum der Deutschen Post. Dort gab es innerhalb eines Zeitraums von 10 Monaten insgesamt 250 Meldungen von Kunden wegen des Verlusts von Briefsendungen. Der Betriebsrat hatte zweimal anlässlich konkreter Verdachtsmomente gegen einzelne Arbeitnehmer der vorübergehenden Installierung einer verdeckten Videokamera zugestimmt. Dadurch konnten die Täter jeweils überführt werden. Bundesweit wurden durch den Einsatz stationärer Videoanlagen in Briefverteilzentren im Jahr 2005 insgesamt elf Täter überführt. Nachdem sich die Betriebsparteien im Jahr 2005 nicht auf die Einrichtung einer stationären Videoüberwachungsanlage verständigen konnten, wurde von der daraufhin angerufenen Einigungsstelle mit der Stimme des Vorsitzenden eine Betriebsvereinbarung zum Einsatz einer stationären Videoanlage beschlossen. Diese Betriebsvereinbarung sieht die Möglichkeit der Videoüberwachung im Innen- und Außenbereich vor. Im Instanzenzug hob das Bundesarbeitsgericht (BAG) die Betriebsvereinbarung insoweit auf, als darin auch eine verdachtsunabhängige Ausweitung der Videoüberwachung auf weitere Betriebsteile vorgesehen war, sofern die Maßnahme in dem Bereich, dem ein konkreter Verdacht zugeordnet werden konnte, zu keinem Erfolg geführt hatte.

Das BAG wiederholte, dass die Betriebsparteien grundsätzlich befugt sind, in einem Betrieb eine Videoüberwachung einzuführen. Allerdings müssen sie dabei den Verhältnismäßigkeitsgrundsatz wahren. Dazu getroffene Regelungen müssen geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen sein, um den erstrebten Zweck zu erreichen. Die Regelung zur Ausweitung der Überwachung ist nach Auffassung des BAG nicht verhältnismäßig. Als Begründung für die Ausdehnung reiche es nicht, dass die Videoaufzeichnung

des zuvor überwachten Bereichs nicht zur Überführung des Täters geführt habe. Damit würde allein die Erfolglosigkeit des bereits vorliegenden Eingriffs in Persönlichkeitsrechte einer geringeren Zahl von Arbeitnehmern zum Grund für weitergehende Eingriffe in die Rechte einer weit größeren Zahl von Arbeitnehmern gemacht. Alle Arbeitnehmer müssten besorgen, dass ohne ihr Wissen nicht nur einzelne Bereiche des Betriebes, in denen der Verdacht einer strafbaren Handlung aufgetreten sei, sondern der gesamte Betrieb überwacht werde. Dies sei unangemessen und verstoße gegen § 6 b Abs. 1 Bundesdatenschutzgesetz (BDSG), weil danach eine Videoüberwachung nur zulässig sei, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen.

C. Datenschutz und Datensicherheit im rbb

I. Aktuelle IT-Projekte

1. Neues Dispositionssystem

Wie in meinen letzten Tätigkeitsberichten ausgeführt, ist seit längerem ein neues einheitliches Dispositionssystem für Hörfunk und Fernsehen geplant, das die bisherigen Systeme ablösen soll. Nachdem das Feinkonzept unter Berücksichtigung der von mir eingebrachten datenschutzrechtlichen Aspekte erstellt war, hat die Geschäftsleitung Anfang 2009 Verhandlungen mit dem Personalrat über eine Dienstvereinbarung aufgenommen.

An den Verhandlungen, bei denen es hauptsächlich um Aspekte des Gesundheitsschutzes und des Datenschutzes geht, nehme ich regelmäßig teil.

2. Urlaubs- und Fehlzeitenverwaltungssystem

In meinem letzten Bericht hatte ich über die Einführung eines Urlaubs- und Fehlzeitenverwaltungssystem berichtet. Die Erfahrungen der letzten Monate haben gezeigt, dass es noch einigen Nachbesserungsbedarf – unter anderem auch zur Verbesserung des Datenschutzes – gibt. Die Projektleitung ist mit dem Personalrat und mir im Gespräch über die erforderlichen Änderungen und Verbesserungen und die entsprechende Überarbeitung der Dienstvereinbarung. Für die sog. Beauftragten, die von den Kolleginnen und Kollegen mit der Beantragung von Urlaub bevollmächtigt werden können, und für die sog. Fehlmelder (Personen, die Krankheitszeiten ins System eingeben) gibt es nun doch – wie von mir gefordert – nur noch eingeschränkte Zugriffsrechte.

3. CAFM-Software

Im Frühjahr 2008 wurde ich darüber informiert, dass im **rbb** und im ARD-Hauptstadtstudio die Absicht bestehe, ein CAFM (Computer Aided Facility Management) - System einzuführen.

Bei der CAFM-Software handelt es sich um eine modulbasierte Standardsoftware für die infrastrukturellen Aufgabenbereiche des Gebäudemanagements. Eine solche Software bietet die Möglichkeit, alle Daten, die für das Facility Management von Belang sind, in einem Datenpool zu vereinen, um auf deren Basis Entscheidungen treffen zu können und die Aufgaben des Facility Managements Ressourcen schonend und effektiv zu erledigen. Bislang wurden die erforderlichen Daten in verschiedenen Systemen vorgehalten (u. a. SAP, Excel, Access).

Das System besteht aus den Modulen Flächenmanagement, Umzugsmanagement, Reinigungsmanagement, Schließmanagement, Instandhaltungsmanagement und Trassenmanagement. Folgende Mitarbeiterdaten werden in dem System verarbeitet: Name, Vorname, Personalnummer, Kostenstelle und Eintritts- und Aus-

trittsdatum und Kontaktdaten. Name und Vorname sowie Kostenstelle dienen der Belegungsplanung, und dazu, einen schnellen Überblick über die aktuelle Belegung von Flächen zu bekommen. Die Felder Eintritts- und Austrittsdatum (sofern diese Felder in SAP in berechtigten Ausnahmefällen – z. B. Kündigung – gefüllt sind) dienen der Abteilung Infrastruktur zur strategischen Planung. So können über diese Daten Sanierungs-, Renovierungs- und Umzugsplanungen besser koordiniert werden. Die Personalnummer dient als interner Zuordnungsschlüssel, um die Daten in das CAFM-System integrieren zu können. Sie wird in der CAFM-Software weder angezeigt noch ausgedruckt.

Durch ein differenziertes Berechtigungskonzept ist sichergestellt, dass die Nutzer des Systems tatsächlich nur auf diejenigen Daten zugreifen können, die sie für ihre Arbeit benötigen. Grundsätzlich können die personenbezogenen Daten nur eingesehen werden. Die Möglichkeit der Veränderung von Daten im CAFM-System ist nur einigen wenigen Personen vorbehalten.

Alle Zugriffe der mit dem System arbeitenden Mitarbeiterinnen und Mitarbeiter werden vom System protokolliert und für Datensicherheitszwecke für den Zeitraum von 30 Tagen gespeichert. Eine Auswertung der Daten durch die Erstellung von Nutzer- bzw. Anwenderprofilen ist unzulässig.

Der Datenkatalog, die Art der Datenauswertung, die Speicherdauer und das Berechtigungskonzept wurden mit mir gemeinsam festgelegt.

In dem Zeitraum September bis November 2008 wurde die Software an die Anforderungen des **rbb** angepasst und installiert. Momentan werden die Module Flächenmanagement und Instandhaltung Bau genutzt. Weiterhin sind die Module Reinigungsmanagement und Schließmanagement installiert. Hier wird in einem nächsten Schritt die Datenübernahme aus den Alt-Systemen durchgeführt. Die Nutzung des Moduls Instandhaltungsmanagement durch die Versorgungstechnik ist für Anfang 2010 geplant.

4. Wireless-LAN-Zugang

Seit Juli 2008 gibt es in sechs Konferenzräumen am Standort Potsdam die Möglichkeit, über ein Wireless-LAN (WLAN = drahtloses lokales Funknetz) in das **rbb**-Netzwerk zu gelangen. Für externe Mitarbeiter und Firmen ist über das WLAN ein Internet-Anschluss gegeben. In die Planungen war ich von Anfang an mit einbezogen. Zusammen mit dem Systemverantwortlichen für IT-Sicherheit habe ich die Nutzungsbedingungen für die Nutzung des WLAN durch Externe entworfen. Darin wird auf den Umstand, dass der Zugang zum Internet unverschlüsselt direkt ins Internet erfolgt, hingewiesen. Aus diesem Grund wird der Einsatz einer AntiVirus- und Personal-Firewall-Software dringend empfohlen. Mit der Anerkennung der Nutzungsbedingungen erklären sich die externen Nutzer damit einverstanden, dass die Verbindungsdaten zur Sicherstellung des ordnungsgemäßen Betriebs und zur Aufklärung etwaiger Missbrauchsfälle protokolliert und für maximal sechs Monate gespeichert werden. Sie erhalten ihre Zugangsberechtigung für die WLAN-Nutzung (Benutzername und Passwort) über ihren **rbb**-Ansprechpartner von dem zuständigen Bereich Informations- und Kommunikationsdienstleistungen (IuKD). Nach dem Einrichten des Accounts werden dem Benutzer die Zugangsdaten an die angegebene Kontaktadresse geschickt bzw. direkt übergeben.

Der Zugang zum **rbb**-Netzwerk via WLAN ist ausschließlich mit **rbb**-Laptops möglich. Die Laptops werden so konfiguriert, dass die **rbb**-Nutzer sich im **rbb**-Netz via WLAN authentifizieren können. Der Schlüssel für die Kodierung ist nur den **rbb**-Administratoren bekannt. Außerdem müssen die Geräte vorher durch IuKD registriert werden. Die Nutzung des WLANs mit privaten Geräten ist nicht erlaubt. Inzwischen gibt es auch in den Konferenzräumen und Foyers in Berlin WLAN.

5. Digitales Produktionssystem (DPS)

Im September 2008 fiel der Startschuss für den Probebetrieb für das neue Digitale Produktionssystem Fernsehen (DPS). Mit diesem System, für das ich – wie üblich - eine datenschutzrechtliche Vorabprüfung durchgeführt habe, ist das vernetzte

Arbeiten der Redaktionen an den unterschiedlichen Standorten möglich, sodass z. B. gleiches Rohmaterial für unterschiedliche Beiträge genutzt werden kann, ohne dass Bandtransporte notwendig sind.

Zu jedem Videoclip werden im System inhaltlich und technisch beschreibende Daten, die sog. Metadaten, gespeichert. Diese dienen der Beschreibung des Materials und werden beim Einspielen von Rohmaterial bzw. beim Überspielen der fertig geschnittenen Beiträge am Schnittplatz eingegeben. Im Web-System kann dadurch nach den entsprechenden Schlagworten gesucht, gesichtet und abgenommen werden. Die Meta-Daten unterfallen als journalistische Daten dem Medienprivileg, so dass für die Verarbeitung der personenbezogenen Daten keine gesonderte Rechtsgrundlage erforderlich ist.

Generell erfolgt im DPS keine Pflege und Aufbewahrung von persönlichen Nutzerdaten. Die Nutzerverwaltung erfolgt über die zentrale **rbb**-Nutzerverwaltung (LDAP). Die Anmeldung an das System kann bei entsprechender Berechtigung von jedem Arbeitsplatz-PC aus erfolgen. Im System werden für alle Prozesse Log-Dateien geschrieben und für Datensicherheitszwecke für maximal 30 Tage gespeichert. Zugriff auf diese Dateien hat nur ein eingeschränkter Kreis an DPS-Administratoren. Die Fernwartung erfolgt durch externe Firmen über VPN nach den Vorgaben unserer „Richtlinien für den Einsatz von Externen bei der Wartung von IT- und TK-Systemen".

6. Neues Sendeplanungssystem Fernsehen (NSF)

Beim **rbb** wird es ein neues Sendeplanungssystem (NSF) für das Fernsehen geben. Dieses neue System ist eine komplexe Softwareanwendung, die den Planungsprozess von der Idee zur Sendung über die Phasen Bewilligung, Anmeldung, Freigabe bis hin zur Sendung und die Sendenachbereitung steuert und unterstützt. NSF kommuniziert über verschiedene Softwareschnittstellen mit einer Vielzahl beim **rbb** eingeführter Systeme, u. a. SAP, FESSAD, dem Videotextsystem, **rbb**-online und der

Fernseh-Sendeautomation. NSF ist ein strategisches Kerninstrument der Programmplanung und der Sendeabwicklung und dient auch als Rechercheinstrument.

Bestandteil der beim Software-Entwickler in Auftrag gegebenen Leistungen war auch ein Datenschutzkonzept, das in Abstimmung mit mir entstanden ist. Während für die Datenhaltung der personenbezogenen Inhaltsdaten (insbesondere der Urheber und Mitwirkenden an TV-Produktionen) das sog. Medienprivileg gilt, unterliegt die Verarbeitung der Nutzerdaten den üblichen Restriktionen. Die Festlegungen, welche Daten der Nutzer überhaupt erhoben werden, orientieren sich – wie üblich - an dem Grundsatz der Datensparsamkeit. Auf die sog. Log-Dateien haben ausschließlich die Administratoren zum Zwecke der Fehleranalyse Zugriff. Die Speicherdauer beträgt drei Monate. Nach Ablauf dieser Frist wird die Datei automatisch gelöscht. Nachdem auch der Systemverantwortliche für IT-Sicherheit keine sicherheitstechnischen Bedenken hatte, konnte ich der Aufnahme des Probebetriebs im Frühjahr 2009 zustimmen.

7. Elektronische Bearbeitung und Archivierung von Rechnungen (eBar)

Beim **rbb** ist die Einführung eines Systems zur elektronischen Bearbeitung und Archivierung von Rechnungen (eBar) geplant. Mit der Einführung dieses Verfahrens soll die papiergebundene Rechnungsprüfung und –archivierung durch eine elektronische ersetzt werden. Durch das elektronische Prüfungsverfahren entfallen Versand- sowie Liegezeiten in der Poststelle. Außerdem ist für das Rechnungswesen jederzeit ersichtlich, wo sich die Rechnung im Prüfungsverfahren gerade befindet. Auf die elektronisch abgelegte Rechnung können Rechnungswesen und Fachabteilungen bei Bedarf jederzeit zugreifen. Dadurch reduzieren sich Rechercheaufwand und Kopierkosten. Auf Grund der Erfahrungen mit der elektronischen Rechnungsbearbeitung soll zu einem späteren Zeitpunkt geprüft werden, ob die Digitalisierung weiterer derzeit papiergebundener Geschäftsvorgänge im **rbb** sinnvoll ist. Somit hat das Projekt innerhalb des Senders auch Pilotcharakter.

In die Planungen von eBar bezieht mich die Projektleitung regelmäßig mit ein. Schwerpunkte meiner Beratung sind zum einen der Schutz der Daten der Mitarbeiterinnen und Mitarbeiter des **rbb**, die mit dem System arbeiten, und zum anderen der Schutz der Daten der Geschäftspartner, soweit es sich dabei um personenbezogene Daten handelt. Der Datenkatalog wird ebenso mit mir abgestimmt wie z. B. das Berechtigungskonzept und die Löschfristen, die sich nach den einschlägigen Regelungswerken des **rbb** (z. B. die Dienstanweisung für die Bearbeitung und Verwaltung von Dokumenten und Akten) richten.

II. SAP-Systeme

1. Release-Wechsel nach ERP 6.0

Am 30. Juni 2008 fand der Release-Wechsel von der Version 4.7 nach SAP ERP 6.0 statt. Dieser Wechsel war notwendig, weil SAP die Wartung für die alte Version eingestellt hat. Datenschutzrechtliche Probleme sind dabei nicht aufgetreten, weil eine 1:1-Umstellung erfolgt ist. Die neuen Funktionalitäten, die das System bietet, sind laut Auskunft der Kollegen in den zuständigen Fachbereichen nicht nutzbar, weil kein entsprechendes Customizing erfolgt ist und die nötigen Berechtigungen nicht vergeben wurden.

2. Umsetzung der Löschfristen

Wie schon in meinem letzten Tätigkeitsbericht erwähnt, ist mir seit Mai 2007 bekannt, dass die SAP-Dienstvereinbarungen hinsichtlich der Löschfristen bislang nicht vollständig umgesetzt worden sind. Der Grund liegt darin, dass eine automatische Löschung von einzelnen Daten aus sog. Infotypen innerhalb eines Stammsatzes technisch überhaupt nicht möglich ist. Möglich ist ausschließlich die automatische Löschung eines kompletten Stammsatzes mit der Folge, dass gar keine Daten über eine bestimmte Person mehr im System vorhanden sind. Dieses Problem ist insbesondere bei dem SAP-Personaldatenverarbeitungs-Modul HR virulent.

Da das händische Löschen einzelner Daten einen unverhältnismäßigen Aufwand bedeuten würde, prüft die zuständige Fachabteilung nun ein elektronisches Werkzeug, mittels dessen die automatische Löschung größerer Datensätze möglich sein soll. Ein Ergebnis liegt bislang noch nicht vor.

III. Datenschutz beim Online-Angebot des rbb

Wie schon in meinem letzten Bericht erwähnt, hat eine Unterarbeitsgruppe des Arbeitskreises von ARD, ZDF und Deutschlandradio unter meiner Leitung einen Leitfaden zum Thema „Datenschutz und Datensicherheit in Sozialen Netzwerken im web 2.0 der Rundfunkanstalten" erarbeitet, der inzwischen vom AK DSB beschlossen wurde. Er ist meinem Bericht als Anlage beigefügt. Der Leitfaden gilt u. a. für sämtliche Online-Angebote des **rbb**.

IV. Arbeitnehmerdatenschutz

1. Allgemeines

Vor dem Hintergrund der bekanntgewordenen fragwürdigen Überwachungsmethoden bei Lidl, Aldi, Deutscher Bahn und Deutscher Telekom haben mich von verschiedenen Kollegen Fragen zur Situation im **rbb** erreicht.

Beim **rbb** existiert ein engmaschiges Netz an Regelungen zum Arbeitnehmerdatenschutz, die in Ergänzung zu den einschlägigen Datenschutzgesetzen wie z. B. dem Berliner Datenschutzgesetz und dem Telekommunikationsgesetz, zur Anwendung kommen. Dazu gehören u. a. die Datenschutz-Dienstanweisung, die Dienstvereinbarung über die Einführung und Anwendung des Telekommunikationsanlagenverbundes (DV TKAV), die Dienstanweisung für die Nutzung von Internet und E-Mail und die Dienstanweisung für die Nutzung des E-Mail-Systems Lotus Notes.

Grundsätzlich kann die Aussage getroffen werden, dass der **rbb** – in den meisten Fällen in Gestalt der Hauptabteilung Personal – all die personenbezogenen Daten zu seinen Mitarbeitern sammeln und verarbeiten darf, die für die Abwicklung des Beschäftigungsverhältnisses nötig sind – also etwa Zeugnisse, Weiterbildungsnachweise, die Adresse, die Kontoverbindung und die Fehltage wegen Krankheit (§ 2 Abs.2 Berliner Datenschutzgesetz i.V.m. § 28 Abs. 1 Nr. 1 Bundesdatenschutzgesetz).

Darüber hinaus darf der **rbb** auch solche personenbezogenen Mitarbeiterdaten verarbeiten, die zur Wahrung seiner berechtigten Interessen erforderlich sind, wenn „kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Mitarbeiters an dem Ausschluss der Verarbeitung oder Nutzung überwiegt" (§ 2 Abs. 2 Berliner Datenschutzgesetz i.V.m. § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz). Dazu gehören beispielsweise Auswertungen von Krankheitstagen ebenso wie Datenauswertungen im Zusammenhang mit Strukturuntersuchungen. Selbstverständlich kommt dem Grundsatz der Verhältnismäßigkeit in diesem Zusammenhang eine ganz besondere Bedeutung zu. Die Mittel-Zweck-Relation muss gewahrt sein. Das jeweilige Interesse des Arbeitgebers und die geplante Maßnahme sind im jeweiligen Einzelfall gegen den Eingriff in das Persönlichkeitsrecht des Arbeitnehmers abzuwägen. Vorrang hat stets eine Auswertung anonymisierter bzw. pseudonymisierter Daten, soweit dies möglich ist.

Nach der Rechtsprechung des Bundesarbeitsgerichts ist eine heimliche Überwachung bzw. Auswertung von Daten nur ausnahmsweise zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zulasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind und die verdeckte Maßnahme praktisch das einzige verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist. Die einschlägigen Bestimmungen in den genannten **rbb**-Regularien entsprechen dieser höchstrichterlichen Rechtsprechung.

2. Interne Leistungsverrechnung

Im Juni 2007 hat der **rbb** ein Einführungsprojekt zur Internen Leistungsverrechnung (ILV) gestartet. Ziel der ILV ist es vor allem, mehr Transparenz und damit ein höheres Kostenbewusstsein im **rbb** zu schaffen. Alle Vorgänge im Haus kosten Geld und sollen damit einen Wert haben. Die ILV soll interne und externe Leistungen gleich behandeln und bewerten. Dazu wird ein interner Markt für Dienstleistungen etabliert. Jährlich sollen Preise für bestimmte Personal- und Sachleistungen festgelegt werden. Für die Abrechnung sollen die anonymisierten Dispositionsdaten aus verschiedenen Systemen bzw. Excel/Access-Dateien zugeliefert werden. Der Personalrat hat im Zusammenhang mit der ILV inzwischen umfangreiche Beteiligungsrechte reklamiert. An den Gesprächen zwischen Projektleitung und Personalrat u. a. zu Fragen der Datenerhebung und –auswertung bin ich beteiligt.

3. Datenschutz bei diversen Mitarbeiterbefragungen

Seit einiger Zeit erfreuen sich elektronische Mitarbeiterbefragungen unter Zuhilfenahme des Programms HelpMatics Survey unseres E-Mail-Systems Lotus Notes im **rbb** großer Beliebtheit. Ich habe mich davon überzeugt, dass die Anonymität bei dem Einsatz von HelpMatics Survey gewahrt ist und habe der Durchführung von einfachen Befragungen mit Hilfe dieses Systems zugestimmt. In einem Fall ging es um die Auswertung von Erfahrungen in den sog. bimedialen Erprobungsfeldern, in dem anderen Fall um die Qualität der Mitarbeiterversorgung in den beiden Kantinen am Standort Berlin.

Einer Online basierten Wahl des Redakteursausschusses im Dezember 2008 konnte ich hingegen meine Zustimmung nicht erteilen. Die Gründe waren folgende: Nicht alle Wahlberechtigten – dazu gehören ja auch die arbeitnehmerähnlichen Personen – verfügen über einen eigenen account beim **rbb**. Die Durchführung einer

kombinierten elektronischen und Papierwahl wäre organisatorisch kaum möglich gewesen. HepMatics Survey ist zwar geeignet, anonyme Abstimmungen durchzuführen, jedoch nicht, revisionssicher auch Wahlen abzubilden.

Ende 2008 informierte mich der Personalratsvorsitzende über eine seinerzeit bereits gestartete Fragebogen-Aktion, die die Electronic Media School (ems) im Auftrag für das Inforadio durchführte. Unklarheiten gab es zum Zweck der Umfrage, zur Freiwilligkeit der Beteiligung und zur Art der Datenverarbeitung. Auf meine Nachfrage beim Chefredakteur von Inforadio erfuhr ich, dass die Umfrage im Zusammenhang mit einem 1/2-jährigen Projekt zur Programmentwicklung stand. Die ems hatte als Austausch- und Kommunikationsplattform für dieses Projekt eine eigene Website eingerichtet.

Eine gänzlich anonyme Durchführung der Befragung war technisch nicht möglich, weil ohne namentliche Zuordnung Mehrfachbeantwortungen nicht hätten ausgeschlossen werden können. Mit dem Chefredakteur und den Verantwortlichen bei der ems einigte ich mich schließlich auf ein Verfahren, bei dem ausschließlich der Administrator der Website und ein weiterer Mitarbeiter der ems Zugang zu den Originaldaten (ausgefüllte Fragebögen in Verbindung mit Namen der Absender) hatten. Beide sicherten in einer schriftlichen Erklärung vertrauliche Behandlung der Namen der Absender zu. Die Auswertung der Ergebnisse wurde anonym an InfoRadio weitergegeben. Die Mitarbeiterinnen und Mitarbeiter wurden ordnungsgemäß über den Zweck der Datenerhebung und die Verarbeitung der Daten informiert.

4. Online-Buchungen bei der Deutschen Bahn AG

Im **rbb** gibt es seit einiger Zeit die Überlegung, über ein Online-Buchungssystem der Deutschen Bahn AG Onlinebuchungen von Bahnfahrkarten zu realisieren. Hintergrund ist die Tatsache, dass das Reisebüro, über das der **rbb** – wie mehrere andere Rundfunkanstalten – bislang die Bahn- und Flugtickets für Dienstreisen seiner Mitarbeiterinnen und Mitarbeiter bezieht, seine Serviceentgelte erhöht hat.

Die Verhandlungen sind schon deshalb seit einiger Zeit ins Stocken geraten, weil die Deutsche Bahn AG vom **rbb** schon vor Vertragsschluss den Abschluss einer sehr restriktiven Geheimhaltungsvereinbarung mit Vertragsstrafeversprechen verlangt. Außerdem sind noch eine Reihe von datenschutzrechtlichen Fragen und Details zum Datensicherheitskonzept zu klären.

5. Briefgeheimnis auch am Arbeitsplatz

Im Berichtszeitraum war ich mit einem Konflikt befasst, bei dem es um Fragen des Briefgeheimnisses am Arbeitsplatz ging. Für eine Mitarbeiterin, die in einen anderen Tätigkeitsbereich gewechselt war, waren während ihres Urlaubs Briefe an ihren alten Arbeitsplatz gesandt worden. Die Briefe waren an sie in ihrer alten Funktion adressiert gewesen. Dabei war nicht eindeutig ersichtlich, dass es sich um persönliche Post handelte. Die Briefe waren von ihrem Nachfolger im Amt geöffnet und über eine dritte Mitarbeiterin an die Kollegin weitergeleitet worden.

Zu der dagegen von der Kollegin erhobenen Beschwerde nahm ich wie folgt Stellung: Gemäß § 32 Abs. 1 der **rbb-**Geschäftsordnung müssen als persönlich gekennzeichnete Eingänge grundsätzlich ungeöffnet an den Adressaten weitergeleitet werden. Sind Briefe an eine Person unter Nennung ihrer Funktion gerichtet und ist diese Funktion inzwischen mit einer anderen Person besetzt, so darf die Nachfolgerin/der Nachfolger die Post während des Urlaubs der Person öffnen, um festzustellen, ob die entsprechenden Schreiben an die Adressatin/den Adressaten persönlich oder aber an die entsprechende Funktionsträgerin/den Funktionsträger gerichtet sind. Im Falle von persönlicher Post ist diese ungelesen direkt an die Adressatin/den Adressaten weiter zu leiten.

V. Sonstiges

1. DTV4all – Digital Television for All

Seit dem 01. Juli 2008 läuft das Europäische Projekt „DTV4all – Digital Television for All". Bei dem auf 30 Monate angelegten Projekt geht es darum, Maßnahmen zur Barrierefreiheit für die alternde Bevölkerung und zur sozialen Integration zu fördern mit dem speziellen Ziel, Zugänge für digitale audiovisuelle Systeme („AV-Systeme") zu entwickeln. DTV4all vereint acht Partner aus Dänemark, Deutschland, Großbritannien, Italien und Spanien. Es widmet sich im Wesentlichen dem Testen unterschiedlicher Technologien für verbesserte Barrierefreiheit im digitalen Fernsehen. In vier Regionen, darunter Berlin-Brandenburg, werden mehrmonatige Tests mit Nutzern durchgeführt. Der **rbb** testet insbesondere die Untertitelung im digitalen Fernsehen, es sind auch sog. „Clean Audio" Tests vorgesehen (Optimierung der Tonspur für Hörgeschädigte). Die Tests werden im Hinblick auf die Nutzerfreundlichkeit und die Machbarkeit neuer technischer Lösungen ausgewertet. Am Ende des Projekts stehen Empfehlungen an die entsprechenden europäischen Institutionen und Vereinigungen mit dem Ziel, zur Standardisierung und europaweiten Verbreitung getesteter barrierefreier Technologien beizutragen. Zusammen mit den **rbb**-Mitarbeitern des Projekts habe ich den Text der datenschutzrechtlichen Einwilligungserklärung entworfen und für die Auswertung der Angaben der Probanden ein Verfahren verabredet, das die Anonymität wahrt.

2. Anfrage zur Nutzung von Lotus-Notes am heimischen PC

Ein Kollege wandte sich mit folgender Frage an mich:

Im Zusammenhang mit der Einrichtung eines Zugangs für seinen heimischen PC für das Lotus-Notes-System des **rbb** via Web durch einen neuen, sog. Web-SSL-Zugang müsse laut Auskunft des Supports eine Software auf seinem PC installiert werden. Er befürchte nun, dass damit persönliche Daten ausgelesen werden können. Auf

Nachfrage beim Systemverantwortlichen für IT-Sicherheit erhielt ich dazu folgende Auskunft, die ich an den Kollegen weitergab:

Die IT-Systeme, die sich über das Internet am **rbb**-Datennetz anmelden möchten, müssen identifiziert werden, damit sichergestellt werden kann, dass keine Schadsoftware über diesen Weg ins **rbb**-Netz gelangt. Dazu wird beim Verbindungsaufbau zwischen Web-Gateway und Client auf dem Client eine Überprüfungs- und Verbindungssteuerungssoftware, der Hostchecker, installiert. Dieser hat folgende Aufgaben:

1. Es werden Angriffe von anderen infizierten Computern aus demselben Netzwerk, in dem sich der Client befindet, blockiert.
2. Es wird verhindert, dass sich Schadsoftware vom Client über das Web-Gateway ins **rbb**-Datennetz verbreitet.

Der Hostchecker ist mit einem Antivirenschutz zu vergleichen, der nur während der Verbindung zum Web-Gateway aktiv ist. Es ist technisch ausgeschlossen, dass dabei lokale Daten vom Client zum **rbb** übertragen werden.

VI. Informationsmaßnahmen

Am 21. August 2008 habe ich wieder zusammen mit einem Kollegen aus der IT-Technik ein zweistündiges Datenschutzseminar für die neuen Auszubildenden durchgeführt. Ziel dieser Veranstaltung war es, die Auszubildenden für die Themen Datenschutz und Datensicherheit zu sensibilisieren.

VII. Sonderarbeitsgruppe „Maßnahmepaket zur Erhöhung der Teilnehmerdichte in Berlin“

Der **rbb** leidet bekanntlich unter massiven Ertragsausfällen, weil überdurchschnittlich viele Menschen in seinem Sendegebiet von der Rundfunkgebühr befreit sind oder sie trotz Pflicht aus unterschiedlichen Gründen nicht zahlen. Auf Bitten der Länder hat sich die KEF im Jahr 2008 mit diesem Problem befasst und den Ministerpräsidenten vorgeschlagen, die ARD solle dem **rbb** zunächst mit einem Darlehen helfen. Die KEF schlug außerdem vor, der **rbb** müsse Maßnahmen entwickeln, mit denen er seine besonders geringe Anmeldequote (sog. Teilnehmerdichte) in Berlin erhöhen kann. Die Ministerpräsidenten sind diesem Vorschlag einstimmig gefolgt. Die Geschäftsleitung hat deshalb Ende 2008 eine Sonderarbeitsgruppe eingesetzt, die das Maßnahmepaket bis zum 30. Juni 2009 erstellen sollte. Als Zielmarke erhielt die Arbeitsgruppe die Vorgabe, dass der **rbb** innerhalb eines Jahres die Teilnehmerdichte in Berlin um einen Prozentpunkt steigert. Die AG unter der Leitung von Petra Schmitz (Sendeleitung und Programmkoordination Fernsehen) tagte von Mitte Februar 2009 an regelmäßig. Sie analysierte die Probleme, befragte Mitarbeiterinnen und Mitarbeiter, informierte sich über das Vorgehen anderer ARD-Anstalten und erarbeitete Vorschläge zur Verbesserung der Gebührensituation des **rbb**. Ich gehörte der Arbeitsgruppe in meiner Funktion als Mitarbeiterin des Justitiariats und als Datenschutzbeauftragte an.

Insbesondere bei den Themenfeldern „Beauftragtendienst“ und „Datenbereitstellung“ habe ich datenschutzrechtliche Aspekte eingebracht.

Während sich viele Ideen als realisierbar herausgestellt haben, z. B. zielgruppengerechte Mailingmaßnahmen und der Einsatz mobiler Datenabfragegeräte durch die Rundfunkgebührenbeauftragten, mussten andere Ideen u. a. aus datenschutzrechtlichen Gründen verworfen werden. So kam z. B. ein Abgleich aller Mitarbeiterdaten mit dem Datenbestand bei der GEZ zur Überprüfung, ob sich alle **rbb**-Mitarbeiter bei der GEZ angemeldet haben, von vornherein nicht in Betracht.

D. Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung

I. Allgemeines

Seit dem 01. Januar 1976 zieht die GEZ die Rundfunkgebühren für die Landesrundfunkanstalten ein. Der bei der GEZ geführte Rundfunkteilnehmer-Datenbestand umfasste per Ende Dezember 2008 rund 39,6 Millionen Teilnehmerkonten mit insgesamt angemeldeten rund 43, 1 Millionen Hörfunkgeräten und 36, 9 Mio. Fernsehgeräten (davon gebührenpflichtig 39,4 Mio. Hörfunk- und 33,5 Mio. Fernsehgeräte, gebührenbefreit 3,7 Mio. Hörfunk- und 3,4 Mio. Fernsehgeräte).

Für den **rbb** stellen sich die Zahlen per 31.12.2008 wie folgt dar:

2.829.667 Teilnehmerkonten, 2.955.972 Hörfunkgeräte (davon befreit 385.296), 2.662.459 Fernsehgeräte (davon befreit 388.467) und 16.875 Neuartige Geräte (davon befreit 565).

Die Überwachung des Datenschutzes bei der Verarbeitung der Rundfunkteilnehmerdaten obliegt der bzw. dem für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten. Für Radio Bremen, den Hessischen Rundfunk und den **rbb** ist zusätzlich der jeweilige Landesdatenschutzbeauftragte zuständig. Unbeschadet der Zuständigkeit des nach Landesrecht für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ist bei der GEZ gemäß § 8 Abs. 2 Satz 2 RGebStV eine betriebliche Datenschutzbeauftragte bestellt. Die betriebliche Datenschutzbeauftragte der GEZ arbeitet zur Gewährleistung des Datenschutzes mit dem/der nach Landesrecht für die jeweilige Rundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese/n über Verstößе gegen Datenschutzvorschriften sowie über die dagegen getroffenen Maßnahmen.

Bei der Rundfunkteilnehmerdatenverwaltung sind meine ständigen Ansprechpartner zum einen die Abteilung Rundfunkgebühren, zum anderen die GEZ in Köln. Während mit der Abteilung Rundfunkgebühren für gewöhnlich Einzelfälle zur

Diskussion stehen, konzentriert sich die Zusammenarbeit mit der GEZ auf die Sicherstellung der datenschutzrechtlichen Unbedenklichkeit des von dieser abzuwickelnden Massenverfahrens.

II. Auskunftsersuchen und Eingaben

Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung und Beantwortung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten 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 2008 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	07
Fragen bzgl. der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung	17
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen	23
Verlangen, Teilnehmerdaten nicht zu anderen Zwecken zu nutzen bzw. zu übermitteln	02
Anfragen von Finanzämtern nach Daten (insbes. Bankverbindungen) von Rundfunkteilnehmern	00
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Rundfunkteilnehmern	03
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz	17
Anzahl der Vorgänge insgesamt:	**69**

Ich selbst habe in 2008 folgende Vorgänge bearbeitet:

Beschwerden über die Vorgehensweise eines Rundfunkgebührenbeauftragten	03
Fragen im Zusammenhang mit der Glaubhaftmachung der Befreiungsvoraussetzungen	10
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz	06
Anzahl der Vorgänge insgesamt:	**19**

Im Vergleich zum Vorjahr (insgesamt 77 Anfragen und Beschwerden aus dem Sendegebiet des **rbb**) ist wieder ein leichter Anstieg zu verzeichnen.

III. NP-Datenbank

Wie berichtet, hatte die GEZ im Jahr 2007 den Probebetrieb mit der NP-Datenbank aufgenommen. Dabei hat sich herausgestellt, dass die auf § 8 Abs. 4 RGebStV beruhende generelle Löschfrist von 12 Monaten entgegen der ursprünglichen Einschätzung der GEZ – offenbar zu kurz ist. Eine Unterarbeitsgruppe, an der sich seitens der Rundfunkdatenschutzbeauftragten die Datenschutzbeauftragten von NDR und RB beteiligten, erarbeitete daraufhin eine Regelung, wonach aus datenschutzrechtlichen Gründen die regelmäßige Löschung der NP-Daten nach einem Jahr zu erfolgen hat und nur bei Vorliegen besonderer Voraussetzungen im Einzelfall eine längere (vierjährige) Speicherung vorgenommen werden kann. Diesen Vorschlag hat sich der AK DSB in seiner Sitzung am 17./18. April 2008 zueigen gemacht.

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

In meinem letzten Tätigkeitsbericht habe ich über die Prüfung der GEZ durch die Landesdatenschutzbeauftragten von Bremen, Hessen, Berlin und Brandenburg am 07. und 08. Februar 2008 berichtet. In ihrem am 09. Oktober 2008 vorgelegten Bericht weisen die Landesdatenschutzbeauftragten auf einige nach ihrer Einschätzung bestehende datenschutzrechtliche Defizite hin. Die Einschaltung des Inkasso-Unternehmens Creditreform zur Realisierung von durch die Finanzämter nicht beigetriebenen Forderungen wurde ausdrücklich als zulässig anerkannt. Anregungen zur Überarbeitung der Verträge mit der Firma Creditreform wurden inzwischen von den Rundfunkanstalten aufgegriffen und befinden sich in der Umsetzung.

V. Datenschutzprüfung bei der Fa. Creditreform Mainz am 30. März 2009

Im Auftrag der GEZ bzw. der Landesrundfunkanstalten führt die Fa. Creditreform in Mainz das Inkasso ausstehender Rundfunkgebührenforderungen durch. Bleiben Vollstreckungsmaßnahmen der Rundfunkanstalten bei den Rundfunkteilnehmern erfolglos, versucht die Firma Creditreform in Abstimmung mit den Landesrundfunkanstalten und der GEZ die säumigen Schuldner doch noch zur Zahlung zu bewegen. Als für den Standort zuständiger Rundfunkdatenschutzbeauftragter führt der Datenschutzbeauftragte des SWR regelmäßig zeitgleich mit der Revision der GEZ Datenschutzkontrollen bei der Fa. Creditreform durch. Der datenschutzrechtlichen Prüfung am 30. März 2009 habe ich mich erstmals angeschlossen.

Die Fa. Creditreform beschäftigt Dritte mit der Wartung ihrer IT-Infrastruktur. Sowohl der Vertrag zwischen den Landesrundfunkanstalten und der Creditreform, als auch die Verträge zwischen der Fa. Creditreform und den externen Firmen werden derzeit um spezifische datenschutzrechtliche Regelungen ergänzt.

Seit 2007 bietet die Fa. Creditreform Runfunkschuldnern Online-Kommunikation über ihr Internet-Portal an. Insbesondere mit Blick auf die Hacker-Problematik habe ich den Geschäftsführer um Prüfung von Verbesserungsmöglichkeiten für das Datensicherheitskonzept gebeten.

VI. Mobile Datenabfragegeräte für die Rundfunkgebührenbeauftragten

Aus Datensicherheitsgründen hat der **rbb** bislang – anders als inzwischen alle anderen Landesrundfunkanstalten – den Einsatz mobiler Datenabfragegeräte durch die Rundfunkgebührenbeauftragten untersagt. Ergibt sich bei den Besuchen der Rundfunkgebührenbeauftragten vor Ort Aufklärungsbedarf, z. B. in Fällen, in denen Personen behaupten, sie seien unter einer anderen Adresse bei der GEZ registriert, so muss der Beauftragte bislang in der Abteilung Rundfunkgebühren bzw. bei seinem sog. Hauptbeauftragten anrufen, um die entsprechenden Informationen zu erhalten. Im Sinne der Effizienz wird nun angestrebt, den Beauftragten die Möglichkeit einzuräumen, vor Ort selbst mittels eines mobilen Datenabfragegerätes in der GEZ-Datenbank zu recherchieren.

Anfang 2009 haben der Leiter der Abteilung Rundfunkgebühren, der Systemverantwortliche für IT-Sicherheit und ich gemeinsam ein Konzept für den Einsatz von mobilen Endgeräten erarbeitet. Danach ist beabsichtigt, interessierten Beauftragten sog. Blackberry-Geräte leihweise zur Verfügung zu stellen. Die Konfiguration der Geräte soll durch den **rbb** erfolgen. Wie gesetzlich vorgeschrieben, haben wir auch die Landesdatenschutzbeauftragten von Brandenburg und Berlin in unsere Planungen einbezogen. Am 13. März 2009 hat ein erstes Gespräch dazu stattgefunden. Der Abstimmungsprozess dauert noch an.

E. Datenschutz im Informationsverarbeitungszentrum (IVZ)

Beim **rbb** wird als Gemeinschaftseinrichtung des Deutschlandradios, des MDR, des NDR, RB, **rbb** und SR das rechtlich unselbstständige Informations-Verarbeitungs-Zentrum (IVZ) betrieben. Dort werden für die beteiligten Anstalten zentral Aufgaben der elektronischen Datenverarbeitung abgewickelt.

Für die Kontrolle des Datenschutzes und der Datensicherheit sind die Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Ohne eine entsprechende rechtliche Verpflichtung ist beim IVZ auch ein betrieblicher Datenschutzbeauftragter bestellt.

Am 03. Juni 2008 fand beim IVZ das jährliche Treffen der Datenschutzbeauftragten der beteiligten Anstalten und des IVZ statt, um datenschutzrechtliche Details zu erörtern. Bei dieser Gelegenheit berichtete der Geschäftsführer Herr Dr. Greten über die schon in meinem letzten Bericht erwähnte Zertifizierung des IVZ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).

F. Datenschutz im ARD-Hauptstadtstudio (HSB)

Im ARD-Hauptstadtstudio, für das ich als ortsansässige Rundfunkdatenschutzbeauftragte für das Tagesgeschäft federführend zuständig bin, gab es im zurückliegenden Jahr keine nennenswerten Themen mit datenschutzrechtlicher Relevanz. Seit Sommer 2008 läuft zwar das Projekt TKS09 (neues Telekommunikationssystem für das HSB), jedoch konnten die Verantwortlichen sich bislang im Rahmen der Planung an den bestehenden internen Regelungen orientieren. Vereinbart ist, dass die Projektleitung mich ab Beginn der Detailplanungsphase, voraussichtlich im Herbst 2009, einbeziehen wird.

.

G. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) ist im Berichtszeitraum zweimal – am 17./18. April 2008 beim Westdeutschen Rundfunk in Münster und am 23./24. Oktober 2008 beim Südwestrundfunk in Mannheim – zusammengekommen. Außerdem fanden drei Telefonschaltkonferenzen (am 08. September und am 16. Dezember 2008 sowie am 03. Februar 2009) statt.

Nach dem plötzlichen Tod unseres Vorsitzenden, des Rundfunkdatenschutzbeauftragten des NDR, Herrn Merten, am 30. Juli 2008 hat die Vorsitzendenfunktion zunächst der Datenschutzbeauftragte der Deutschen Welle kommissarisch übernommen. Auf der Oktober-Sitzung in Mannheim hat mich der AK DSB ab dem 01. Januar 2009 für zwei Jahre zur Vorsitzenden gewählt. Die Datenschutzbeauftragte des Bayerischen Rundfunks, Frau Barbara Nickel, ist meine Stellvertreterin.

Schwerpunkte unserer Beratungen waren u.a. die gesetzliche Vorratsdatenspeicherung, Datenschutz und Datensicherheit im Web 2.0, die Verwendung von IP-Adressen für die Medienforschung, das Lösch- und Speicherkonzept der NP-Datenbank bei der GEZ, die Umsetzung des gesetzlichen Auskunftsanspruchs nach den Landesdatenschutzgesetzen, virtuelle Telefonanlagen, der Umgang mit Altdaten von SRT und ZFP durch den gemeinsamen Rechtsnachfolger, die ARD-ZDF-Medienakademie, Fragen im Zusammenhang mit dem Zugriff von Mitarbeitern von kommerziellen Tochterunternehmen (Werbe- und Vermarktungstöchter) der Rundfunkanstalten auf die Programmarchive, der Prüfbericht der Landesdatenschutzbeauftragen sowie die Datensicherheitspanne beim gemeinsamen Kinderkanal von ARD und ZDF KIKA.

Der AK DSB hat die Kollegin des NDR - wie schon in den Vorjahren - auch im Jahr 2008 damit betraut, ihn in der Datenschutzarbeitsgruppe nach Art. 29 EG-Datenschutzrichtlinie zu vertreten. In seiner Sitzung am 23./24. Oktober 2008 hat er diesen Auftrag für das Jahr 2009 verlängert. Der AK DSB wird durch den NDR regelmäßig über die Tätigkeiten und Initiativen der Art. 29-Arbeitsgruppe informiert.

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. Als ständiges beratendes Mitglied vertrete ich den AK DSB in diesem Gremium.

Das IT-Sicherheitsgremium hat im Berichtszeitraum insgesamt dreimal getagt: am 07. Mai 2008 beim ORF in Wien, am 10. September 2008 beim WDR in Köln und am 11. Februar 2009 beim HR in Frankfurt am Main. Themen waren u. a. ein IT-Sicherheitsaudit im ARD-CN, die Datensicherheit beim Video-File-Transfer, eine beim MDR durchgeführte Risikoanalyse der mobilen Hörfunk-Produktionsnetze, die Behandlung von IT-Sicherheitsvorfällen im ARD-CN, Einzelfragen zum Freigabeverfahren für Anwendungen im ARD-CN und das externe Hosting von TK-Anlagen.

III. Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern

Im Arbeitskreis Medien diskutieren die Datenschutzbeauftragten von Bund und Ländern unter dem Vorsitz der Brandenburgischen Datenschutzbeauftragten, 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 Arbeitskreises der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten teil. Der AK DSB hat den Datenschutzbeauftragten des Südwestrundfunks, Herrn Prof. Armin Herb, mit dieser Aufgabe betraut. Als die Rundfunk-Datenschutzbeauftragte vor Ort werde auch ich regelmäßig zu den Sitzungen des AK Medien eingeladen.

Am 10. November 2008 haben Herr Prof. Herb und ich ein ausführliches Gespräch mit Frau Hartge in deren Behörde in Kleinmachnow geführt. Wir haben vereinbart, die Zusammenarbeit von AK Medien und AK DSB zu intensivieren. Frau Hartge wird künftig regelmäßig an einem Teil der Sitzungen des AK DSB teilnehmen. Die wechselseitige Einbringung von eigenen Themenvorschlägen zur Tagesordnung des jeweiligen anderen Arbeitskreises wurde vereinbart.

Am 17. Februar 2009 haben Prof. Herb und ich zusammen an der Sitzung des AK Medien in Potsdam teilgenommen. Themen waren u. a. die Handy-Ortung im Notfall, die Entwicklung von „Voice over IP" in den Ländern, die Online-Archive der Medien und das Recht auf Resozialisierung, Anonymisierungsdienste nach der Vorratsdatenspeicherung, das Recht auf anonymen Fernsehempfang beim digitalen Fernsehen und diverse Einzelpunkte zum Thema Rundfunkgebühreneinzug.

IV. Teilnahme an Veranstaltungen

Europäischer Datenschutztag

Unter dem Titel „Die ideale Angestellte, der genormte Arbeitnehmer. Wie viel darf mein Arbeitgeber über mich wissen?" fand am 28. Januar 2009 in Berlin anlässlich des 3. Europäische Datenschutztages eine Veranstaltung des Bundesdatenschutzbeauftragten statt, an der ich teilgenommen habe. Vor dem Hintergrund der Enthüllungen der Datenschutzverstöße bei der Telekom, der Deutschen Bahn AG und anderer großer Unternehmen erhielt das Thema eine ganz besondere Aktualität. Die Teilnehmer der Podiumsdiskussion (Detlef Scheele, Staatssekretär im Bundesministerium für Arbeit und Soziales, Michael Sommer, Vorsitzender des DGB, Prof. Peter Gola, Vorstandsvorsitzender der Gesellschaft für Datenschutz und Datensicherheit, Prof. Dr. Peter Wedde, Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der Fachhochschule Frankfurt/Main und Dr. Alexander Dix, Datenschutzbeauftragter des Landes Berlin) waren sich einig in der Empörung

über die extensiven Überwachungspraktiken der Firmen. Kontrovers wurde die Frage nach der Notwendigkeit eines Arbeitnehmerdatenschutzgesetzes diskutiert. Zwar sind die Arbeitnehmerdatenschutzrechte bereits heute ganz überwiegend kodifiziert, jedoch mangelt es an der Übersichtlichkeit, da sich die einzelnen Vorschriften in ganz unterschiedlichen Regelungswerken wie z. B. im BDSG, im TKG, im AGG und in den Personalvertretungsgesetzen finden und im Übrigen auch viele Details durch die Rechtsprechung festgelegt sind. Ich persönlich würde die Schaffung eines Arbeitnehmerdatenschutzgesetzes begrüßen.

Berlin, 12. August 2009

gez. Anke Naujock

Anlage