7. Tätigkeitsbericht

der Beauftragten für den Datenschutz
des
Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2009 bis 31. März 2010

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

Inhaltsverzeichnis

Vorbemerkung

Meine Tätigkeit im Berichtszeitraum war im Wesentlichen geprägt von den mit meiner Funktion als Vorsitzende des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) zusammenhängenden Aufgaben. Ich habe dieses Amt seit Anfang 2009 und noch bis zum Ende 2010 inne. Im Berichtszeitraum fanden zwei reguläre Sitzungen des Arbeitskreises statt. Daneben gab es Telefonschaltkonferenzen und Sitzungen im kleineren Kreis zu einzelnen Themen. Im Mittelpunkt standen Themen rund um den Rundfunkgebühreneinzug. Auch mit ersten Modellüberlegungen zum neuen Rundfunkbeitragsstaatsvertrag waren wir Rundfunkdatenschutzbeauftragten relativ früh befasst.

Dem stellvertretenden behördlichen Datenschutzbeauftragten, Herrn Dr. Bismark, danke ich für seine Unterstützung, insbesondere bei den Vor- und Nachbereitungen der Sitzungen des AK DSB. Mit seinem juristischen Sachverstand und seinen langjährigen Erfahrungen in der Arbeit in unterschiedlichen ARD-Gremien war er für mich stets ein kluger Berater im Hintergrund. Auch bei meiner Kollegin im Sekretariat, Frau Ruthild Just, möchte ich mich für ihren besonderen Einsatz im Berichtszeitraum bedanken. Das Organisatorische war bei ihr in besten Händen. Schließlich möchte ich auch in diesem Jahr wieder dem Systemverantwortlichen für IT-Sicherheit, Herrn Gerry Wolff, für die konstruktive Zusammenarbeit danken. Mit dem Personalrat hatte ich einen weiteren engagierten Mitstreiter für den Datenschutz an meiner Seite.

Förmliche Beanstandungen waren auch in diesem Berichtszeitraum nicht auszusprechen. Soweit es in Einzelfällen zu Verletzungen von Datenschutzbestimmungen gekommen ist, wurde den Empfehlungen der Datenschutzbeauftragten in den Fachbereichen umgehend gefolgt.

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

Im Nachfolgenden soll ein kurzer Überblick über die Entwicklungen im Bereich des Datenschutzrechts auf europäischer und nationaler Ebene während des Berichtszeitraums mit Relevanz für den **rbb** gegeben werden.

I. Europa

1. Änderung der EU-Datenschutzrichtlinie für elektronische Kommunikation im Rahmen des sog. Telekom-Reformpakets

Ende 2009 wurde nach einem mehrjährigen Diskussions- und Beratungsprozess von EU-Parlament und EU-Kommission das sog. Telekom-Reformpaket beschlossen. Das Paket umfasst die Änderung von insgesamt fünf Richtlinien für eine europäische Telekommunikationsrahmengesetzgebung. Ein Kernbestandteil des neuen Rechtsrahmens ist dabei die Reform der Richtlinie über den Datenschutz in der elektronischen Kommunikation (sog. ePrivacy-Richtlinie) mit dem Ziel eines verbesserten Schutzes der Verbraucher vor Datenschutzverletzungen und Spams. Die Privatsphäre der europäischen Bürger ist nach Aussage von EU-Kommissarin Reding eine der Prioritäten des neuen europäischen Telekommunikationsrechts.

Telekommunikationsbetreiber und Internet-Diensteanbieter müssen die Namen, E-Mail-Adressen und Kontoangaben ihrer Kunden, vor allem aber auch die Verkehrsdaten über jeden Anruf und jede Internetsitzung sicher aufbewahren, damit diese nicht zufällig oder absichtlich in falsche Hände gelangen können. Die Betreiber müssen die volle Verantwortung für die Verarbeitung und Speicherung solcher Informationen übernehmen. Deshalb wird bei Datenschutzverletzungen eine neue Benachrichtigungspflicht eingeführt – die erste derartige Vorschrift in Europa. Demnach werden Kommunikationsunternehmen die Behörden und ihre Kunden über Sicherheitsverletzungen, die personenbezogene Daten betreffen, informieren müssen. Dies steigert die Anreize für die Betreiber von Kommunikationsnetzen und –diensten, personenbezogene Daten besser zu schützen.

Darüber hinaus werden die Vorschriften über die Wahrung der Privatsphäre und den Datenschutz verstärkt und z. B. auf „Cookies“ und ähnliche Techniken ausgedehnt. So müssen die Internetnutzer besser über den Einsatz von „Cookies“ und den Umgang mit personenbezogenen Daten informiert werden und können in der Praxis leichter über ihre persönlichen Informationen bestimmen. Ferner erhalten Internet-Diensteanbieter neue Rechtsmittel zum Schutz ihres Unternehmens und ihrer Kunden vor Spam-Versendern.

Auf Ebene der Verbraucherrechte gilt künftig, dass Werber für das automatisierte Versenden ihrer Reklamebotschaften per E-Mail, Fax, SMS oder MMS sowie für maschinelle Marketinganrufe eine vorherige Zustimmung der Kunden einholen

müssen. Dazu kommt der Anspruch auf einen Anbieterwechsel bei Erhalt einer Telefonnummer innerhalb eines Arbeitstages oder die Begrenzung maximaler Vertragslaufzeiten auf zwei Jahre.

Das gesamte Telekom-Reformpaket ist mit seiner Veröffentlichung im EU-Amtsblatt am 18. Dezember 2009 in Kraft getreten und ist nun bis Juni 2011 in die nationale Gesetzgebung in den 27 EU-Mitgliedstaaten umzusetzen.

2. 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 wegen der Einrichtung unabhängiger Datenschutzstellen vor dem EuGH berichtet. Mit Urteil vom 09.03.2010 hat der EuGH festgestellt, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 der EU-Datenschutzrichtlinie verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit" wahrnehmen, falsch umgesetzt hat.

Europarechtswidrig ist nach Auffassung des EuGH nicht nur die organisatorische Einbindung zahlreicher Landesdatenschutzbehörden für den nichtöffentlichen (= privaten) Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden.

Das EuGH-Urteil bezieht sich ausdrücklich auf die Kontrollstellen für den privaten Bereich. Zu den Datenschutzkontrollstellen für den öffentlichen Bereich (öffentliche Verwaltung, öffentlich-rechtliche Rundfunkanstalten, Kirchen etc.) hat sich der EuGH nicht geäußert.

Überprüfungs- und Änderungsbedarf aufgrund des Urteils besteht also in erster Linie bei den Bundesländern, die den Datenschutz für den privatwirtschaftlichen Bereich nicht bei den Landesdatenschutzbeauftragten mit angesiedelt haben, sondern innerhalb der Ministerien. In Brandenburg ist mit Wirkung zum 1. Juni 2010 das Brandenburgische Datenschutzgesetz geändert worden. Die Brandenburgische Datenschutzbehörde ist danach nun nicht mehr nur – wie bisher – für die Kontrolle der Datenverarbeitung in der öffentlichen Verwaltung, sondern jetzt auch für den privaten Bereich zuständig. In Berlin gibt es diese Doppelzuständigkeit des Landesdatenschutzbeauftragten seit vielen Jahren.

Für den öffentlich-rechtlichen Rundfunk hat das Urteil keine unmittelbaren Auswirkungen. Im Gegenteil bestätigen die Ausführungen des EuGH zur Unabhängigkeit der datenschutzrechtlichen Kontrollstellen von staatlichen Stellen und politischer Einflussnahme das Konzept, die Rundfunkdatenschutzbeauftragten als Kontrollstellen im Sinne von Art. 28 Abs. 1 EU-Datenschutzrichtilinie einzurichten, die lediglich der Dienstaufsicht der Gremien unterstehen und in Ausübung ihres Amtes unabhängig und nur dem Gesetz unterworfen sind.

Angesichts der in der Praxis kaum durchzuführenden Trennung des wirtschaftlich-administrativen vom journalistisch-redaktionellen Tätigkeitsbereich ist auch eine gespaltene Zuständigkeit für die Datenschutzkontrolle bei den öffentlich-rechtlichen Rundfunkanstalten, wie sie derzeit beim Hessischen Rundfunk, bei Radio Bremen und beim **rbb** existiert, abzulehnen. Insoweit lässt sich aus dem Urteil (wie auch aus dem aus Artikel 5 Grundgesetz abgeleiteten Gebots der Staatsferne des öffentlich-rechtlichen Rundfunks) die Bekräftigung der Forderung ableiten, die datenschutzrechtliche Kontrolle bei den öffentlich-rechtlichen Rundfunkanstalten ausschließlich den Rundfunkdatenschutzbeauftragten zu überantworten.

II. Bund

1. Gesetzgebung

a) Bundesdatenschutzgesetz

Der Bundestag hat 2009 zahlreiche Änderungen des Bundesdatenschutzgesetzes beschlossen – die sogenannten BDSG-Novellen I,II und III. Sie haben unterschiedliche Themenschwerpunkte und sind zu jeweils unterschiedlichen Zeitpunkten in Kraft getreten. Auslöser für diese Gesetzesinitiative waren die sich in der jüngeren Vergangenheit häufenden Datenskandale (u. a. wurden Kontoverbindungsdaten gehandelt und haben mehrere große Unternehmen Gesundheitsdaten von Arbeitnehmern rechtswidrig verarbeitet). Diese Vorfälle waren zwar auch nach bisheriger Rechtslage unzulässig und sanktionierbar, trotzdem sind sie – nicht zuletzt aufgrund des öffentlichen Drucks – zum Anlass genommen worden, weit reichende Einschränkungen durchzusetzen.

aa) BDSG-Novelle I

Zum 01. April 2010 ist die BDSG-Novelle I in Kraft getreten. Wesentliches Ziel des Gesetzgebers war es, die Tätigkeit von Auskunfteien und ihrer Vertragspartner (insbesondere Kreditinstitute) transparenter zu machen, indem Informations- und Auskunftsrechte von Betroffenen gestärkt werden. Des Weiteren enthält das Gesetz spezifische Erlaubnistatbestände und Regelungen für das Scoringverfahren. Dies sind mathematisch-statistische Verfahren zur Berechnung der Wahrscheinlichkeit eines bestimmten Verhaltens, insbesondere zur Kreditwürdigkeit einer Person. Der Gesetzgeber hat dazu zwei völlig neue Tatbestände - § 28 a Datenübermittlung an Auskunfteien und § 28 b Scoring – geschaffen.

bb) BDSG-Novelle II

In der Neufassung des § 3a BDSG ist der Grundsatz der Datenvermeidung und Datensparsamkeit über den Systemdatenschutz hinaus auf alle Erhebungen, Ver-

arbeitungen und Nutzungen personenbezogener Daten erstreckt worden. Wenn die Möglichkeit zur Anonymisierung oder Pseudonymisierung besteht, so ist sie schon unter Erforderlichkeitsgesichtspunkten zu nutzen, solange dadurch kein unverhältnismäßiger Aufwand entsteht. Wie schon bislang muss bei der Auswahl und Herstellung von Softwareprodukten darauf geachtet werden, dass diese so wenig personenbezogene Daten verarbeiten wie möglich.

Die Rechtsstellung des betrieblichen Datenschutzbeauftragten wurde in Bezug auf den Kündigungsschutz und den Anspruch auf Fort- und Weiterbildung gestärkt (§ 4 f BDSG).

Es wurden erweiterte Anforderungen an die Auftragsdatenverarbeitung in § 11 BDSG festgelegt. Die Neufassung des § 11 BDSG regelt nun in einem detaillierten Zehn-Punkte-Katalog die Mindestanforderungen für den Inhalt des schriftlich erteilten Auftrags. Er entspricht weitestgehend bereits der von den Aufsichtsbehörden geforderten Praxis. Unter anderem ist auch die Pflicht des Auftraggebers zu Kontrollen der Einhaltung beim Auftragnehmer vor und während des Outsourcings mit entsprechender Dokumentation zu regeln.

Am meisten umstritten war das ursprüngliche Vorhaben des Gesetzgebers, die Nutzung der Daten für Adresshandel und Marketingzwecke stets an eine ausdrückliche Einwilligung zu knüpfen. Die nun beschlossene Regelung stellt einen Kompromiss dar zwischen den Maximalforderungen von Daten- und Verbraucherschützern einerseits und den Argumenten der Werbe- und Informationswirtschaft sowie deren Kunden andererseits. Die schwer verständlich formulierte Neuregelung in § 28 Abs. 3 BDSG sieht nun eine Abstufung vor: Grundsätzlich können nur mit einer Einwilligung des Betroffenen, die bestimmten formalen Kriterien entsprechen muss, sämtliche personenbezogenen Daten gehandelt werden (sog. „opt-on"-Regelung). Nach wie vor gilt aber für verschiedene Ausnahmefälle das sog. Listenprivileg, wonach listenmäßig oder sonst zusammengefasste Daten, die für bestimmte eigene Zwecke erhoben wurden, für andere Zwecke (z.B. Werbezwecke) genutzt oder an Dritte übermittelt werden dürfen. Im Einzelnen gelten für die Listendaten folgende Ausnahmen von der „opt-in"-Regelung:

- Für eigene Angebote darf gegenüber Bestandskunden oder unter Nutzung von Daten aus allgemein zugänglichen Verzeichnissen (wie Telefonbüchern) geworben werden.
- Berufsbezogene Werbung bleibt erlaubt.
- Die Werbung zwischen Unternehmen bleibt erlaubt.
- Steuerbegünstigte Organisationen dürfen weiterhin für Spenden werben.
- Die Übermittlung von Adressen (mit Angabe einer Gruppenzugehörigkeit) ist zudem zulässig, wenn eindeutig aus dem Werbeschreiben hervorgeht, wer die Datenquelle ist, wer also die Daten erstmals gespeichert hat. Dies muss auch in nachprüfbarer Form dokumentiert sein.

Zulässig ist auch die Nutzung von Daten zur Werbung für fremde Angebote, wenn die für die Nutzung verantwortliche Stelle eindeutig erkennbar ist. Zusätzlich soll ein Koppelungsverbot (vgl. § 28 Abs. 3b BDSG) zukünftig verhindern, dass Unternehmen den Abschluss von Verträgen von der Zustimmung in die Verarbeitung der Daten abhängig machen. Betroffene haben wie schon bisher das Recht, der werblichen Verwendung ihrer Daten zu widersprechen (vgl. § 38 Abs. 4 BDSG). Damit hat der Gesetzgeber in der ersten Stufe zwar dem „opt-in" den Vorzug gegeben, gestattet aber die Beibehaltung der bisherigen Verfahrensweisen unter der Voraussetzung, dass Datenherkunft und Datenempfänger bekannt gegeben werden bzw. für Kontrollzwecke aufgedeckt werden können. Für die Daten, die bis zum 31. August 2009 erhoben und verarbeitet wurden, gelten die alten Regelungen noch bis zum 31. August 2012. Die Datenverarbeitung für Zwecke der Markt- und Meinungsforschung ist nunmehr in einer eigenen Vorschrift § 30a BDSG geregelt.

Neu hinzugekommen ist die Regelung des § 32 BDSG, welche erstmals eine ausdrückliche Bestimmung zum Beschäftigtendatenschutz enthält. Er tritt an die Stelle des § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Die nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebende Zweckbestimmung wird für das Beschäftigungsverhältnis dahin konkretisiert, dass Beschäftigtendaten erhoben, verarbeitet oder genutzt werden dürfen, wenn dies im Rahmen der verschiedenen Phasen eines Arbeitsverhältnisses, d. h. seiner Begründung, Durchführung oder Beendigung erforderlich ist. Welche Daten vom Arbeitgeber insoweit benötigt werden, bestimmt

sich nach wie vor anhand der vom BAG entwickelten Kriterien, d. h. unter Beachtung des Verhältnismäßigkeitsprinzips ist das objektive Informationsinteresse des - potentiellen – Arbeitgebers mit dem Anspruch des Beschäftigten auf Persönlichkeitsrechtsschutz abzuwägen. Im Beschäftigungsverhältnis erforderlich sein können auch Maßnahmen, die der Abwehr von Pflichtverletzungen dienen (z. B. Zeiterfassung, offene Videoüberwachung, Taschenkontrolle, Kontrolle rechtmäßiger Internetnutzung etc...)

Sowohl § 33 BDSG (Benachrichtigung) als auch § 34 BDSG (Auskunft) sind geändert worden.

Die Kompetenzen der Aufsichtsbehörden wurden erweitert (vgl. § 38 BDSG). Neben der Befugnis, technische oder organisatorische Mängel selbst zu beseitigen, dürfen die Behörden nun generell formale Anordnungen zur Beseitigung von Datenschutzverstößen aussprechen und bei Nicht-Abschaffung Bußgelder verhängen.

Ebenfalls neu sind die Regelungen zur Informationspflicht bei Datensicherheitsverletzungen in § 42a BDSG. Wird unrechtmäßig Kenntnis von sensiblen Daten erlangt und besteht ein erhebliches Missbrauchsrisiko, so sind die Betroffenen und die Aufsichtsbehörde zu informieren – erforderlichenfalls öffentlich, z.B. durch Anzeigen in bundesweit erscheinenden Tageszeitungen.

Schließlich wurden auch die Bußgeldvorschriften angepasst (vgl. § 43 BDSG): Der Bußgeldrahmen reicht nun bis zu 50.000,- Euro in leichten und 300.000,- Euro in schweren Fällen. Ist der Verletzergewinn höher, kann er über diese Rahmenbeträge hinaus abgeschöpft werden.

Die wesentlichen Änderungen der Novelle II traten bereits zum 01. September 2009 in Kraft. Für die bis dahin erhobenen oder gespeicherten Daten gilt während bestimmter Übergangsfristen (§ 47 BDSG) weiterhin § 28 BDSG in der derzeitigen Fassung.

cc) BDSG-Novelle III

Im Rahmen der BDSG-Novelle III wurden in § 29 Abs. 7 BDSG Auskunftspflichten von Kredit ablehnenden Stellen bei Bonitätsanfragen innerhalb der EU/des EWR verankert. Die Vorschrift regelt in Umsetzung von Art. 9 der Verbraucherkreditlinie den Anspruch des Betroffenen auf Information über eine Datenbankabfrage und greift nur, wenn der Abschluss eines Verbraucherdarlehensvertrages (§ 491 Abs. 1 BGB) oder eines entgeltlichen Finanzierungshilfevertrages (§ 506 BGB) abgelehnt wird.

dd) Bedeutung der Novellierungen des BDSG für den rbb

Für den **rbb** gelten, soweit nicht die spezielleren Vorschriften im **rbb**-Staatsvertrag greifen, die Vorschriften über die Verarbeitung personenbezogener Daten des Landes Berlin (§ 36 **rbb**-Staatsvertrag). Allerdings verweist § 2 Abs. 2 Berliner Datenschutzgesetz für die Datenverarbeitung in Beschäftigungsverhältnissen auf die einschlägigen Vorschriften des Bundesdatenschutzgesetzes. Von Interesse wird überdies sein, ob und inwieweit das Berliner Datenschutzgesetz im Hinblick auf die BDSG-Novellierung angepasst wird. Dies betrifft insbesondere den Punkte-Katalog zur Auftragsdatenverarbeitung in § 11 BDSG.

b) Gesetz über das Verfahren des elektronischen Entgeltnachweises (sog. ELENA-Verfahrensgesetz)

Am 28. 03. 2009 wurde das Gesetz über das Verfahren des elektronischen Entgeltnachweises (sog. ELENA Verfahrensgesetz) zur Änderung der §§ 95ff. des Vierten Buches Sozialgesetzbuch (SGB IV) beschlossen. Das Gesetz ist zum 1. Januar 2010 in Kraft getreten.

Das ELENA-Verfahren soll künftig für eine Vielzahl von Bescheinigungen die Arbeitergeber von der aufwändigen Erstellung entlasten und gleichzeitig das Verfahren für die Antragsteller vereinfachen. Dazu sind die Arbeitgeber seit dem

01. Januar 2010 gesetzlich verpflichtet, monatlich eine entsprechende ELENA-Meldung an die bundesweit zentrale Speicherstelle (ZSS) zu versenden, damit die bisher vom Arbeitgeber auf Papier erstellten Gehaltsbescheinigungen in Verfahren vor Sozialbehören elektronisch zur Verfügung stehen (vgl. § 97 SGB IV).

In der ELENA-Datenbank werden ab dem 01. Januar 2010 Daten gespeichert, die bislang in Antragsverfahren vor Sozialbehörden (Arbeitsagentur, Wohngeldstelle, Elterngeldstelle) auf amtlichen Vordrucken erhoben wurden. Es handelt sich daher um Einkommensdaten und um weitere Angaben, die für die Prüfung notwendig sind, ob ein Anspruch auf die Sozialleistung besteht oder nicht. Die gespeicherten Daten können erst ab dem 01. Januar 2012 von den ausdrücklich dazu befugten Stellen einzelfallbezogen abgerufen werden, sofern der betroffene Antragsteller den Abruf mit seiner individuellen elektronischen Signaturkarte freigegeben hat.

Die Daten werden bei der ZSS in verschlüsselter Form gespeichert. Die Datensätze der Beschäftigten sind dabei nicht unter ihrem Namen, sondern unter einem Pseudonym abgelegt. Der Zugriff auf die Daten und die Zuordnung der Datensätze zu einzelnen Beschäftigten ist nur möglich, wenn der Betroffene die Daten durch die Vorlage seiner Signaturkarte freigibt und zugleich eine gültige Signaturkarte eines Mitarbeiters einer zugriffsberechtigten Stelle vorliegt (Zwei-Schlüssel-Prinzip). Die individuelle Signaturkarte bleibt bei dem betroffenen Bürger. Darüber hinaus sind die Daten verfahrenstechnisch so gesichert, dass diese nur von den Behörden und für deren Aufgaben abgerufen werden können, die gemäß § 99 SGB IV im Verfahren zugelassen wurden. Zugriffe von Arbeitgebern oder Finanzbehörden sowie eine Beschlagnahmung der Daten durch eine Staatsanwaltschaft sind ausgeschlossen.

Die Informationen werden je nach Vorgang bereits jetzt von den Arbeitsagenturen in der Bescheinigung zum Arbeitslosengeld abgefragt. Durch ELENA ändert sich zum einen der Transportweg, zum anderen erfolgt die Speicherung der Daten nun bei einer zentralen Stelle und „auf Vorrat".

Ab 2012 sollen diese Informationen dann für verschiedene Behördenanträge zentral zur Verfügung stehen. Die Nutzung dieser Daten ist bisher auf den Fall beschränkt, dass soziale Leistungen der Bundesagentur für Arbeit sowie der Elterngeld- und Wohngeldstellen beantragt werden. Es ist aber schon jetzt absehbar, dass die Nutzung der Daten künftig auch auf andere Sozialleitungsbereiche ausgeweitet werden soll.

Mit diesem bis vor kurzem in der Öffentlichkeit weitgehend unbeachteten Verfahren des elektronischen Entgeltnachweises wird eine der größten Datensammlungen mit personenbezogenen Daten in Deutschland geschaffen. Datenschützer hatten während des gesamten Entstehungsprozesses daher auch erhebliche Bedenken angemeldet und entsprechende Anforderungen für ein datenschutzkonformes, rechtmäßiges ELENA-Verfahren formuliert. Kurz vor Inkrafttreten zum 01. Januar 2010 ist die Kritik an ELENA auch von den Medien noch einmal aufgegriffen worden. Vor allem ist datenschutzrechtlich bedenklich, dass Einkommensdaten von allen Beschäftigten, Beamten, Richtern und Soldaten zentral gespeichert werden, ohne dass feststeht, ob die Daten im Einzelfall tatsächlich jemals gebraucht werden. Aus diesem Grund wird ELENA von den Datenschutzbeauftragten des Bundes und der Länder sowie anderen Einrichtungen, insbesondere den Gewerkschaften, aber auch Politikern als verfassungswidrige Datenspeicherung auf Vorrat kritisiert.

Kritisiert wurde ursprünglich ferner, dass jeder Streikende in dieser Datenbank erfasst werden sollte, egal ob bei einem offiziellen oder wilden Streik. Erfasst werden sollte auch die Aussperrung. Das Bundesministerium für Arbeit hat hierzu am 05. Januar 2010 mitgeteilt, dass das Verfahren dahingehend geändert worden sei, dass Streikzeiten nicht mehr als solche erfasst werden. Außerdem sollen noch einmal alle zu erhebenden Daten auf ihre zwingende Notwendigkeit hin überprüft werden.

Durch das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung bei der Telekommunikation (siehe dazu 2. a) sehen sich die Gegner von ELENA in ihrer Kritik bestätigt. Nachdem das Urteil zur Vorratsdatenspeicherung verkündet

worden war, initiierten der Arbeitskreis Vorratsdatenspeicherung und der FoeBuD (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V.), innerhalb weniger Tage vor Ablauf der Jahresfrist, auch gegen das ELENA-Verfahren eine Massenklage. Am 31. März 2010 wurden 22.005 Vollmachten nach Karlsruhe transportiert und als Sammelbeschwerde beim Bundesverfassungsgericht eingereicht.

Die Personalräte von ARD, ZDF und Deutschlandsradio haben in einer gemeinsamen Erklärung vom 27. Januar 2010 gegen ELENA protestiert und eine Rücknahme des ELENA-Gesetzes gefordert.

Was bedeutet ELENA für den Rundfunk Berlin-Brandenburg?

Trotz der datenschutzrechtlichen Bedenken ist das ELENA-Gesetz seit dem 01. 01. 2010 in Kraft. Daher muss auch der **rbb** seiner gesetzlichen Verpflichtung nachkommen und monatlich die Daten der Beschäftigten an die ZSS in Würzburg übermitteln - dies jedenfalls solange das Gesetz nicht zurückgenommen wird oder die Klagen dagegen Erfolg haben. Seit Juni 2010 übermittelt der **rbb** rückwirkend ab Januar 2010 die Daten an die zentrale Speicherstelle.

c) Gesetz zur Stärkung der Sicherheit in der Informationstechnik (BSI-Gesetz)

Am 18. 06. 2009 beschloss der Deutsche Bundestag trotz Proteste vieler Bürger gegen die Stimmen von Grünen, FDP und Linke ein „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“. Dieses Gesetz ermächtigt das Bundesamt für Sicherheit in der Informationstechnik erstmals, ohne Anlass Informationen über die elektrische Kommunikation jedes Bürgers mit Bundesbehörden und Bundestagsabgeordneten z. B. per Mail aufzuzeichnen und unter bestimmten Voraussetzungen an Polizei, Verfassungsschutz und Strafverfolgungsbehörden weiterzugeben. Erfasst wird dabei auch jede Nutzung öffentlicher Internetportale von Bundesbehörden, so auch, wer sich wann für welche Internetseiten interessiert hat und nach welchen Worten er dort gesucht

hat. In einer gemeinsamen Stellungnahme von Medieninstitutionen (u.a. ARD), wurde im Vorfeld insbesondere bemängelt, dass bei der Datenweitergabe kein Schutz für die in § 53 StPO geschützten Personengruppen vorgesehen sei. Im Gesetz vom 14.08.2009 (BGBl. S. 2821) ist jetzt aber durch die Einfügung in § 5 Abs. 7 zumindest ein Verwertungsverbot für das Kommunikationsverhalten aller in § 53 Abs. 1 Satz 1 StPO genannten Personen – das sind Personen mit gesetzlicher Schweigepflicht, auch Journalisten verankert worden.

Gegen das BSI-Gesetz ist inzwischen von mehreren Personen Verfassungsbeschwerde erhoben worden.

2. Rechtsprechung

a) Entscheidung des BVerfG zur Vorratsdatenspeicherung vom 02.03.2010

Seit Beginn des Jahrzehnts scheiterten mehrere Versuche, eine Vorratsdatenspeicherung in Deutschland einzuführen, weil der Gesetzgeber darin einen zu starken Eingriff in die Freiheitssphäre sah. Dies änderte sich mit der Richtlinie 2006/24/EG vom 15.03.2006, die eine Vorratsdatenspeicherung von Daten vorsieht, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden. Die Speicherpflicht betrifft genau spezifizierte Verkehrsdaten aller Dienste, die über Festnetze oder Mobilnetze erbracht werden, wie etwa Telefonie, Internettelefonie, Fax, SMS, MMS, E-Mail, Filetransfer, www, Chat und Newsgroups. Diese Daten sind für 6 bis 24 Monate zu speichern. Die Vorratsdatenspeicherung darf ausschließlich zu dem Zweck erfolgen, den zuständigen staatlichen Behörden Zugriff auf die Daten zu ermöglichen, um „schwere Straftaten" zu ermitteln, festzustellen und zu verfolgen. Die Richtlinie war bis zum 15.09.2007, für Internet-Zugang, -Telefonie und –Mail bis zum 15.03.2009 umzusetzen. Nach heftigen Debatten wurde am 21.12.2007 das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" verabschiedet. Es übernahm in § 113 a TKG die Speicherpflichten aus der Richtlinie, beschränkte die entschädigungslose Speicherpflicht der TK-Anbieter auf sechs Monate plus einen

Monat für die Löschung der Daten und legte ihnen für die Datensicherheit „die im Bereich der Telekommunikation allgemein erforderliche Sorgfalt“ auf. Hinsichtlich der Verwendung der Daten gingen § 113 b TKG und § 100g StPO weit über die Vorgaben der Richtlinie hinaus und sahen die Übermittlung der Daten „zur Verfolgung von Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und zur Erfüllung der gesetzlichen Aufgaben“ der Nachrichtendienste vor. Auch erlaubte die Vorschrift, die Daten für Auskünfte über Anschlussinhaber zu nutzen. Die Pläne zur Vorratsdatenspeicherung stießen auf großen Widerstand, die Rechtmäßigkeit der Richtlinie und ihrer deutschen Umsetzung wurden bezweifelt. Vertreter der FDP und von Bündnis 90/Die Grünen sowie einer großen Bürgerinitiative legten Verfassungsbeschwerde mit der bislang größten Zahl von Beschwerdeführern (über 34 000) ein. Das Bundesverfassungsgericht (BVerfG) erließ – wie in meinen früheren Tätigkeitsberichten erwähnt - mehrere einstweilige Anordnungen, mit denen im Wesentlichen die Datenverwendung der zuständigen Behörden auf den Schutz überragend wichtiger Rechtsgüter beschränkt wurde. In seinem am 02.03.2010 verkündeten Urteil hat das BVerfG mit 6:2 Stimmen nun §§ 113 a und 113 b TKG und § 110 g I 1 StPO für nichtig erklärt und angeordnet, die nach diesen Vorschriften gespeicherten Daten unverzüglich zu löschen. Das Gericht wertet die Vorratsdatenspeicherung zwar als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“, hält sie jedoch mit dem in Art. 10 GG verankerten Fernmeldegeheimnis nicht schlechterdings für unvereinbar. Voraussetzung ist, dass sie legitimen Zwecken dient und in ihrer Ausgestaltung „dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt“. Allerdings macht es die verfassungsrechtliche Unbedenklichkeit einer Vorratsspeicherung davon abhängig, dass sie eine Ausnahme bleibt. Eine Gesetzgebung, „die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte, wäre von vornherein mit der Verfassung unvereinbar“. Zukünftig ist eine doppelte Verhältnismäßigkeitsprüfung notwendig: Zum einen ist auf der Grundlage der Wirkungen eines Überwachungsinstruments dessen verhältnismäßiger Einsatz zu bewerten. Zum anderen ist aber zusätzlich auf der Basis einer Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbelastungen bürgerlicher Freiheiten zu prüfen. Danach kann der

Gesetzgeber Überwachungsmaßnahmen eventuell nur austauschen, aber nicht kombinieren. Damit die Vorratsdatenspeicherung verhältnismäßig sein kann, fordert das BVerfG, dass ihre Ausgestaltung dem besonderen Gewicht des Eingriffs angemessen Rechnung getragen wird. Die Verhältnismäßigkeit sieht das BVerfG nur unter den folgenden Bedingungen als erfüllt an:

- Die Vorratsdatenspeicherung bedarf der gesetzlichen Gewährleistung eines besonders hohen Standards der Datensicherheit.
- Der Abruf und die unmittelbare Nutzung der Daten sind angesichts der Schwere des Eingriffs nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen.
- Es muss eine größtmögliche Transparenz gewährleistet sein.
- Es bedarf eines effektiven Rechtsschutzes und effektiver Sanktionen.

Für alle entscheidenden Vorschriften hat das BVerfG festgestellt, dass sie gegen diese verfassungsrechtlichen Vorgaben verstoßen. Die Konsequenz ist, dass die deutschen Umsetzungsregelungen nichtig sind. Eigentlich ist der deutsche Gesetzgeber jetzt aufgefordert, die EU-Richtlinie zügig neu umzusetzen. Allerdings kann man davon ausgehen, dass er sich hier eher Zeit lassen wird. Es gilt, äußerst sorgfältig vorzugehen, um ein erneutes Scheitern vor dem BVerfG zu vermeiden. Außerdem steht die EU-Richtlinie selbst noch auf dem Prüfstand. Der EuGH wird noch die Vereinbarkeit der Richtlinie mit der EU-Grundrechtscharta prüfen. Daher ist es sehr wahrscheinlich, dass ein neuer Regelungsversuch erst nach Vorliegen der Ergebnisse der EU-Diskussion unternommen wird.

b) Beschluss des BVerfG zur Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver eines Providers vom 16. Juni 2009

Dem Beschluss des BVerfG vom 16. 06. 2009 lag folgender Sachverhalt zugrunde:
In einem gegen Dritte gerichteten strafrechtlichen Ermittlungsverfahren wegen Untreue und Betrug sollten bei einer richterlich angeordneten Wohnungsdurchsuchung bei dem Beschwerdeführer Unterlagen und Dateien der Beschuldigten aufgefunden werden. In dem Beschluss hieß es: „Ferner wird gem. §§ 100g, 100h StPO die Auswertung von ggfs. zu beschlagnahmenden Datenträgern gestattet,

insbesondere Textdateien und E-Mail-Verkehr." Der Beschwerdeführer untersagte den Ermittlungspersonen den Zugriff auf sein E-Mailpostfach, weil der Durchsuchungsbeschluss diesen nicht umfasse. Er nutzte für den Zugriff auf seine E-Mails das sog. Internet Message Access Protocol. Hiernach verblieben die empfangenen E-Mails auch nach Abruf auf dem zugangsgesicherten Bereich des Mailserver seines Providers gespeichert, weshalb die Herstellung einer Internetverbindung mit Eingabe des entsprechenden Passwortes erforderlich war. Mit Beschluss ordnete das Amtsgericht daraufhin gemäß §§ 94,98 StPO die Beschlagnahme der E-Mails auf dem Mailserver des Providers an, worauf die gesamten 2.500 E-Mails des späteren Beschwerdeführers auf einen Datenträger kopiert und den Ermittlungsbehörden übergeben wurden. Dagegen erhob der Beschwerdeführer Beschwerde und vertrat die Auffassung, dass eine Anordnung nach § 100a StPO (heimliche Überwachung des Fernmeldeverkehrs) erforderlich gewesen sei, die mangels Verdacht einer Katalogtat nicht habe ergehen können. Das Landgericht verwarf die Beschwerde. Gegen die Beschlüsse des Amtsgerichts und des Landgerichts wendete sich der Beschwerdeführer mit seiner Verfassungsbeschwerde.

Der Zweite Senat des Bundesverfassungsgerichts hat die Verfassungsbeschwerde zurückgewiesen. Der Senat stellte fest, dass Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers in das Fernmeldegeheimnis des Art. 10 GG eingreifen, im Einzelfall jedoch verfassungsrechtlich zulässig sind. Eine Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails aufgrund § 94 StPO sei verhältnismäßig. Es bedürfe insoweit keines Rückgriffs auf die Normen der § 100a, 100c oder 100g StPO, die eine schwere, besonders schwere oder eine Straftat von erheblicher Bedeutung verlangen. Ansonsten wäre es problemlos möglich, bei geringen Verstößen einfach die entsprechende E-Mail-Korrespondenz dem Zugriff der Strafverfolgungsbehörden durch Auslagerung auf einen E-Mailserver zu entziehen. Soweit die E-Mails von der Ermittlungsbehörde gespeichert und ausgewertet werden, wird dem ihm zustehenden Auskunftsrechts des Betroffenen durch entsprechende Vorschriften in der StPO Rechnung getragen. Des Weiteren müssen die nicht zu dem konkreten Ermittlungsverfahren gewonnenen E-Mails gelöscht bzw. an den Betroffenen herausgegeben werden.

c) Urteile des BGH vom 15. Dezember 2009 zu Online-Archiven und Medienprivileg

Mit zwei Urteilen vom 15. 12. 2009 hat der Bundesgerichtshof (BGH) entschieden, dass die wegen Mordes an einem berühmten Schauspieler zu lebenslanger Freiheitsstrafe verurteilten, inzwischen wieder entlassenen Straftäter nicht vom Deutschlandradio verlangen können, Mitschriften von Rundfunkbeiträgen unter voller Namensnennung aus dem für Altmeldungen vorgesehen Teil des Internetauftritts zu entfernen. Anders als die Vorinstanzen sah der BGH hier einen Unterlassungsanspruch nicht als begründet an.

Im vorliegenden Fall habe das Interesse des Klägers am Schutz seiner Persönlichkeit und an der Achtung seines Privatlebens hinter dem vom Deutschlandradio verfolgten Informationsinteresse der Öffentlichkeit und dem Recht auf freie Meinungsäußerung zurückzutreten. Zwar komme dem Interesse des Klägers, vor einer Reaktualisierung seiner Verfehlung verschont zu bleiben, ein erhöhtes Gewicht zu. Die von ihm begangene Straftat und die Verurteilung liegen lange zurück; er sei im August 2007 aus der Strafhaft entlassen worden. Andererseits beeinträchtige die beanstandete Passage der Mitschrift der Rundfunksendung sein Persönlichkeitsrecht einschließlich seines Resozialisierungsinteresses unter den besonderen Umständen des Streitfalls nicht in erheblicher Weise. Sie sei insbesondere nicht geeignet, ihn „ewig an den Pranger" zu stellen oder in eine Weise „an das Licht der Öffentlichkeit zu zerren", die ihn als Straftäter (wieder) neu stigmatisieren könnte. Die beanstandete Passage enthalte wahrheitsgemäße Aussagen über ein Kapitalverbrechen an einem bekannten Schauspieler, das erhebliches öffentliches Aufsehen erregt hatte. Zum Zeitpunkt der Einstellung der Meldung in den Internetauftritt des Deutschlandradios sei sie unzweifelhaft zulässig gewesen. In der Art und Weise, wie die Mitschrift des Rundfunkbeitrags zum Abruf bereitgehalten wird, komme ihr nur geringe Breitenwirkung zu. Sie sei nur auf den für Altmeldungen vorgesehenen Seiten des Internetauftritts zugänglich und ausdrücklich – und für den Nutzer ohne weiteres ersichtlich – als Altmeldung gekennzeichnet. Zugunsten von Deutschlandradio fiel darüber hinaus ins Gewicht, dass ein erkennenswertes

Interesse der Öffentlichkeit nicht nur an der Information über das aktuelle Zeitgeschehen, sondern auch an der Möglichkeit besteht, vergangene zeitgeschichtliche Ereignisse zu recherchieren. Dementsprechend nehmen die Medien ihre Aufgabe, in Ausübung der Meinungsfreiheit die Öffentlichkeit zu informieren und an der demokratischen Willensbildung mitzuwirken, auch dadurch wahr, dass sie nicht mehr aktuelle Veröffentlichungen für interessierte Mediennutzer verfügbar halten. Diese umfassende Aufgabe der Medien komme beispielsweise in § 11 d Abs. 2 Nr. 4 Rundfunkstaatsvertrag zum Ausdruck, wonach der Auftrag der öffentlich-rechtlichen Rundfunkanstalten auch das Angebot zeitlich unbefristeter Archive mit zeit- und kulturgeschichtlichen Inhalten umfasst. Ein generelles Verbot der Einsehbarkeit und Recherchierbarkeit bzw. ein Gebot der Löschung aller früheren den Straftäter identifizierenden Darstellungen in Online-Archiven würde dazu führen, dass Geschichte getilgt und der Straftäter vollständig immunisiert würde. Das vom Kläger begehrte Verbot würde einen abschreckenden Effekt auf den Gebrauch der Meinungs- und Pressefreiheit haben, der den freien Informations- und Kommunikationsprozess einschnüren würde. Würde auch das weitere Bereithalten ausdrücklich als solcher gekennzeichneter und im Zeitpunkt der Einstellung zulässiger Altmeldungen auf für Altmeldungen vorgesehenen Seiten zum Abruf im Internet nach Ablauf einer gewissen Zeit oder nach Veränderung der zugrunde liegenden Umstände ohne weiteres unzulässig und wäre das Deutschlandradio verpflichtet, sämtliche archivierten Hörfunkbeiträge von sich aus immer wieder auf ihre Rechtmäßigkeit zu kontrollieren, würde die Meinungs- und Medienfreiheit in unzulässiger Weise eingeschränkt. Angesichts des mit einer derartigen Kontrolle verbundenen personellen und zeitlichen Aufwands bestünde die erhebliche Gefahr, dass die Medien entweder ganz von einer der Öffentlichkeit zugänglichen Archivierung absehen oder bereits bei der erstmaligen Sendung die Umstände ausklammern würde, die das weitere Vorhalten der Mitschrift der Sendung später rechtswidrig werden lassen könnten, an deren Zugänglichkeit die Öffentlichkeit aber ein schützenswürdiges Interesse hat. Eine andere rechtliche Beurteilung sei auch nicht nach den Grundsätzen des Datenschutzrechts geboten. Denn das Bereithalten der Meldung unterfalle jedenfalls dem sog. Medienprivileg mit der Folge, dass seine Zulässigkeit weder von einer Einwilligung des Betroffenen, noch von einer ausdrücklichen gesetzlichen Ermächtigung abhängig ist. Das Medienprivileg

sei Ausfluss der in Art. 5 Abs. 1 Satz 2 GG verankerten Rundfunkfreiheit. Ohne die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auch ohne Einwilligung des jeweils Betroffenen wäre journalistische Arbeit nicht möglich. Presse und Rundfunk könnten ihre grundgesetzlich zuerkannten und garantierten Aufgaben nicht wahrnehmen.

Diese Urteile – inzwischen liegen weitere entsprechende Urteile des BGH vor - sind bemerkenswert klar und bringen für die Rundfunkanstalten eine gewisse Entlastung. Allerdings sind sie kein „Persilschein" und beziehen sich jeweils auf den konkreten Einzelfall. Gegen die Urteile ist Verfassungsbeschwerde eingelegt worden.

d) Urteil des BGH zur Rechtmäßigkeit von Bewertungsforen im Internet vom 23. Juni 2009 (www.spickmich.de)

Der Bundesgerichtshof (BGH) hat die Benotung von Lehrern im Internetforum spickmich.de mit Urteil vom 23. 06. 2009 erlaubt. Zwar stünden dem gegen den Provider einer Internetplattform geltend gemachten Anspruch eines Betroffenen auf Löschung bzw. Unterlassung von Bewertungen durch Nutzer weder § 10 Telemediengesetz (TMG) noch § 41 Bundesdatenschutzgesetz (BDSG) entgegen. § 10 TMG betreffe lediglich die strafrechtliche Verantwortlichkeit und die Schadensersatzhaftung des Diensteanbieters. Dies ergebe sich aus der Regelung in § 7 Abs. 2 Satz 2 TMG, wonach die Verpflichtungen zur Entfernung und Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 TMG unberührt bleiben. Wird ein rechtswidriger Beitrag in ein Community-Forum eingestellt, so sei der Betreiber als Störer i. S. v. § 1004 Abs. 1 Satz 1 BGB zur Unterlassung und, wenn nur über die Beseitigung der Daten die Unterlassung durchgesetzt werden kann, zur Löschung verpflichtet. Das Gericht hat sich überdies nicht der in der rechtlichen Diskussion zur Zulässigkeit von Bewertungsforen vertretenen Auffassung angeschlossen, wonach die Vorschriften des BDSG auf die Datenerhebung und –übermittlung in Form eines Bewertungsportals nur eingeschränkt Anwendung fänden, weil für mit Bewertungsforen verbundene Datenerhebungen das in § 41

BDSG enthaltene Medienprivileg gelte. Die sich beispielsweise aus § 41 Abs. 1 BDSG ergebende datenschutzrechtliche Sonderstellung der Medien sei daran gebunden, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten einer pressemäßigen Veröffentlichung dient. Maßgebend sei, dass die Daten „ausschließlich für eigene journalistisch-redaktionelle oder literarische Zwecke" bestimmt sind. Übertragen auf den Bereich der Telemedien könne mithin die reine Übermittlung von erhobenen Daten an Nutzer nicht unter den besonderen Schutz der Presse fallen, weil die bloße automatische Auflistung von redaktionellen Beiträgen noch nicht eine eigene journalistisch-redaktionelle Gestaltung darstelle. Erst wenn die meinungsbildende Wirkung für die Allgemeinheit prägender Bestandteil des Angebots und nicht nur schmückendes Beiwerk ist, könne von einer solchen Gestaltung gesprochen werden. Dennoch sah der BGH den Portal-Betreiber als zur Datennutzung berechtigt an. Bei der Abwägung zwischen dem Schutz des Rechts auf informationelle Selbstbestimmung der klagenden Lehrerin nach Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG und dem Recht auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG des Portalbetreibers sei zu berücksichtigen, dass es sich bei den von dem Portalbetreiber erhobenen und abgespeicherten Bewertungen der Klägerin um Werturteile handele, die ihre Sozialsphäre betreffen. Die Bewertungen betreffen ihre berufliche Tätigkeit, also einen Bereich, in dem sich die persönliche Entfaltung von vornherein im Kontakt mit der Umwelt vollzieht. Äußerungen im Rahmen der Sozialsphäre dürfen nur im Falle schwerwiegender Auswirkungen auf das Persönlichkeitsrecht mit negativen Sanktionen verknüpft werden, so etwa dann, wenn eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung zu besorgen sind. Dies sei hier nicht der Fall. Die Bewertungen stellten weder eine unsachliche Schmähkritik noch eine Formalbeleidigung oder einen Angriff auf die Menschenwürde der Lehrerin dar.

e) Urteil des Bundesarbeitsgerichts vom 23. April 2009 zum Beweisverwertungsverbot bei mitgehörten Telefongesprächen

In dem Urteil des Bundesarbeitsgerichts (BAG) vom 23. 04.l 2009 zugrunde liegenden Fall stritten die Parteien über die Wirksamkeit zweier ordentlicher Arbeitgeberkündigungen. Die Klägerin, deren Arbeitsverhältnis gekündigt worden

war, hatte behauptet, dass ihr Arbeitgeber ihr zuvor in einem Telefonat gedroht hatte, das Arbeitsverhältnis zu kündigen, wenn sie nicht trotz Arbeitsunfähigkeit zur Arbeit erscheint. Den Inhalt dieses Telefonats hätte eine Bekannte ungewollt mit angehört. Sie, die Klägerin habe das ihr nicht vertraute Mobiltelefon ihres Ehegatten benutzt, das von diesem auf maximale Lautstärke eingestellt gewesen sei. Sie habe das Mobiltelefon nicht vom Ohr weggehalten. Wegen des Gesprächsverlaufs sei sie so aufgebracht gewesen, dass sie nicht wahrgenommen habe, dass ihre Bekannte auch die Aussagen ihres Arbeitgebers habe mit anhören können.

Der Inhalt des Telefonats war entscheidungserheblich. Nach § 612 a BGB darf der Arbeitgeber einen Arbeitnehmer nicht deshalb bei einer Maßnahme benachteiligen, weil der Arbeitnehmer in zulässiger Weise seine Rechte ausübt. Als „Maßnahmen" i. S. d. § 612 a BGB kommen auch Kündigungen in Betracht. Ein wegen Krankheit arbeitsunfähiger Arbeitnehmer ist von der Pflicht zur Arbeitsleistung befreit. Er ist berechtigt, der Arbeit fernzubleiben. Droht der Arbeitgeber dem Arbeitnehmer, das Arbeitsverhältnis zu kündigen, wenn der Arbeitnehmer nicht trotz Arbeitsunfähigkeit zur Arbeit erscheint, und kündigt der Arbeitgeber unmittelbar nach der Weigerung des Arbeitnehmers, die Arbeit aufzunehmen, das Arbeitsverhältnis, liegt ein Sachverhalt vor, der eine Maßregelung i. S. d. § 612 a BGG indiziert.

Zunächst hat das BAG in seinem Urteil auf die Rechtsprechung des BVerfG Bezug genommen, wonach das zivilrechtliche allgemeine Persönlichkeitsrecht des Gesprächspartners eines Telefongesprächs verletzt ist, wenn der andere einen Dritten durch aktives Handeln zielgerichtet veranlasst, das Telefongespräch heimlich mitzuhören. Aus der rechtswidrigen Erlangung des Beweismittels folgt ein Beweisverwertungsverbot: Der Dritte darf nicht als Zeuge zum Inhalt der Äußerungen des Gesprächspartners vernommen werden, der von dem Mithören keine Kenntnis hat. Für den Fall, dass ein Dritter zufällig, ohne das der Beweispflichtige etwas dazu beigetragen hat, den Inhalt des Telefonats mithören konnte, stellt es sodann klar, dass in diesem Fall keine Verletzung des zivilrechtlichen allgemeinen Persönlichkeitsrechts des Gesprächspartners vorliege. In diesem Fall bestehe auch kein Verwertungsverbot.

C. Datenschutz und Datensicherheit im rbb

I. Aktuelle IT-Projekte

1. Neues Dispositionssystem

In meinen früheren Tätigkeitsberichten habe ich schon wiederholt darüber informiert, dass beim **rbb** ein neues einheitliches Dispositionssystem für Hörfunk und Fernsehen eingeführt werden soll. Nach langwierigen Verhandlungen zwischen Geschäftsleitung und Personalrat konnte am 09. 11. 2009 endlich der Probebetrieb beginnen. Die Festlegungen zu den datenschutzrechtlichen Rahmenbedingungen des Probebetriebs erfolgten unter meiner Mitwirkung. Nach wie vor befindet sich das Dispositionssystem nicht im Regelbetrieb. Wegen einiger Detailprobleme konnte eine Dienstvereinbarung bislang nicht abgeschlossen werden.

2. Urlaubs- und Fehlzeitenverwaltungssystem

Auch das Thema „Urlaubs- und Fehlzeitenverwaltungssystem" konnte im Berichtszeitraum noch nicht endgültig abgeschlossen werden.

Wie berichtet, haben sich Projektleitung und Personalabteilung auf mein gemeinsam mit dem Personalrat erfolgtes Betreiben dazu bereiterklärt, die bisherigen Erfahrungen in der Anwendung des neuen Systems zu nutzen und zugunsten des Arbeitnehmerdatenschutzes in verschiedenen Punkten von den Festlegungen in der derzeit gültigen Dienstvereinbarung abzuweichen. So gibt es z. B. für die sog. Fehlmelder (Personen, die Krankheitszeiten ins System eingeben) auf meine Forderung hin inzwischen nur noch eingeschränkte Zugriffsrechte. Leider spiegeln sich diese Verbesserungen noch nicht in einer überarbeiteten Dienstvereinbarung wieder. Auf Nachfrage erfuhr ich, dass zunächst die Verhandlungen mit dem Personalrat zu anderen Dienstvereinbarungen abgeschlossen werden sollen, bevor man sich die Dienstvereinbarung zum Urlaubs- und Fehlzeitenverwaltungssystem

wieder vornehme. Das führt dazu, dass ich bei einschlägigen Anfragen von Kollegen zur Verarbeitung ihrer Daten im Urlaubs- und Fehlzeitenverwaltungssystem nicht einfach auf die im Intranet veröffentlichte Fassung der Dienstvereinbarung verweisen kann, sondern Zugriffsrechte und Auswertungen jeweils individuell erläutern muss. Im Sinne der Transparenz wäre es wünschenswert, dass die Dienstvereinbarung schnellstmöglich überarbeitet und wie üblich im Intranet veröffentlicht wird.

3. Neues multimediales Planungs- und Redaktionssystem

Die Redaktionssysteme im **rbb** stoßen mit den neuen Anforderungen der multimedialen Programmdirektion an ihre Grenzen. Deshalb entwickelt der **rbb** seit 2009 ein System, das für Hörfunk, Fernsehen und Online gleichermaßen nutzbar ist. Die Leiter des Projekts „Neues multimediales Planungs- und Redaktionssystem" haben frühzeitig mit dem IT-Sicherheitsbeauftragten und mir Kontakt aufgenommen, um die Anforderungen von Datenschutz und Datensicherheit an das System zu klären.

In dem inzwischen erstellten Leistungsverzeichnis wurde folgenden Forderungen von mir Rechnung getragen:

Das System wird ein Berechtigungskonzept erhalten, bei dem sichergestellt ist, dass die einzelnen Nutzer Zugriffsrechte nur für diejenigen Daten erhalten, die sie für ihre Arbeit brauchen. Dabei wird zwischen lesenden und schreibenden Rechten unterschieden. Die in das System eingegebenen Daten werden jederzeit ihrem Ursprung zugeordnet werden können. Es wird belegbar sein, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Weitergehende Auswertungen, insbesondere Auswertungen, die Rückschlüsse auf das Leistungsverhalten von Mitarbeiterinnen und Mitarbeitern ermöglichen, werden technisch ausgeschlossen. Das System wird die Möglichkeit aufweisen, dass einzelne personenbezogene Daten nach einem vom **rbb** zu definierenden Zeitraum automatisch gelöscht werden. Die Realisierung der sog. Betroffenenrechte insbesondere auf Auskunft, Berichtigung, Sperrung, Löschung (vgl. z. B. § 7 Berliner Datenschutz-

gesetz) wird möglich sein. Zur Wahrung von Informantenschutz und Redaktionsgeheimnis wird es im System sog. geschützte Bereiche geben.

4. Elektronische Bearbeitung und Archivierung von Rechnungen (eBar)

In meinem letzten Tätigkeitsbericht hatte ich über die Planungen zur Einführung eines Systems zur elektronischen Bearbeitung und Archivierung von Rechnungen (eBar) berichtet. Inzwischen befindet sich eBAR im Probebetrieb. Dafür wurde das SAP-Modul FI erweitert.

Nun muss noch die entsprechende Dienstvereinbarung zu SAP FI um die Regelungen für eBAR erweitert werden. Ein entsprechender Änderungsentwurf der Dienstvereinbarung mit einer neuen Anlage mit dem eBAR-Berechtigungskonzept ist mit mir abgestimmt worden. Voraussetzung für die Ordnungsmäßigkeit der Buchführung ist die Zertifizierung dieses Systems durch die Wirtschaftsprüfer. Die Zertifizierung erfolgt auf Grundlage der Verfahrensdokumentation. Diese beinhaltet unter anderem auch das in Abstimmung mit mir erstellte IT Sicherheitskonzept für eBAR. Derzeit erfolgt die Angebotseinholung für die Zertifizierung.

5. Medienbroker

Im Herbst 2009 hat der **rbb** im Rahmen einer Kooperation mit BR und MDR den Probebetrieb für einen sog. Medienbroker eingeführt. Der Medienbroker ist ein Browser basierendes Werkzeug für redaktionelle Recherchen und Materialbestellungen. Der Medienbroker stellt eine einheitliche Rechercheoberfläche mit Vorhör-, Vorschau- und Bestellfunktion für diverse Datenbanken zur Verfügung. Damit ist es möglich, über eine einfach zu bedienende Suchmaske auf mehreren, technisch teilweise sehr unterschiedlichen Systemen parallel eine Recherche auszuführen. Die Recherche wird von sog. Schnittstellen-Agenten auf die Anfragesprache der Systeme übersetzt. Diese Agenten wandeln die Ergebnisse schließlich in HTML um, so dass sie in einem Webbrowser angezeigt und verarbeitet werden können, so wie die Benutzer dies aus dem Internet gewohnt sind. Darunter liegen hauptsächlich Archivdatenbanken. Über die Schnittstellen-Agenten kann der Medien-

broker auch Bestellprozesse in bestimmten Zielsystemen auslösen. Ferner gibt es eine Email-Funktion, die Emails zum Bestellstatus verschickt und bei Fehlern den Administrator alarmiert.

Zusammen mit dem IT-Sicherheitsbeauftragten habe ich die Vorabkontrolle für den Medienbroker durchgeführt. Danach konnte ich meine Zustimmung zum Probebetrieb erteilen. Ausschlaggebend waren folgende Aspekte: Der Nutzerkreis für den Medienbroker ist auf die Journalistinnen und Journalisten beschränkt. Diese Einschränkung ist zur Wahrung des Medienprivilegs unverzichtbar. Da die Applikation zu 95 % nur lesend auf andere Systeme zugreift, ist die Möglichkeit des Datenmissbrauchs gering. Ausschließlich zu Zwecken der IT-Sicherheit werden die notwendigen Verbindungsdaten für eine kurze Dauer gespeichert. Zugriff darauf haben nur die Administratoren. Auch ansonsten wird nur das für den workflow tatsächlich Erforderliche an personenbezogenen Nutzerdaten (Bestellungen) für kurze Zeit gespeichert und anschließend wieder gelöscht.

II. SAP-Dienstvereinbarungen

Im Zuge der Verhandlungen über die neue Dienstvereinbarung zum neuen Dispositionssystem (s. I. Ziff.1) wurden auch die Dienstvereinbarungen zu SAP wieder einer näheren Betrachtung unterzogen, da es zwischen dem Dispositionssystem und SAP verschiedene Schnittstellen gibt. So werden beispielsweise die Stammdaten aus SAP HR ins Dispositionssystem übernommen, die für die Abrechnung der Dienste erforderlichen Daten werden nach SAP Co überspielt.

Bei der Prüfung der Dienstvereinbarungen ist aufgefallen, dass über den durch die Einführung des Dispositionssystems erforderlichen Ergänzungsbedarf weitere Anpassungen stattfinden müssen, die sich u. a. daraus ergeben, dass inzwischen zum Teil andere Anwender mit dem System arbeiten, als in den Dienstvereinbarungen vereinbart, und dass inzwischen – unabhängig vom Dispositionssystem - einige zusätzliche Auswertungen erforderlich geworden sind, die noch nicht in den Dienstvereinbarungen erwähnt sind.

Die Verhandlungen zwischen Geschäftsleitung und Personalrat dazu haben begonnen. Ich werde – wie üblich – einbezogen.

III. Arbeitnehmerdatenschutz

1. Pandemieplan

Die Geschäftsleitung hat in ihrer Sitzung am 07. 08. 2009 die Abteilung Organisation und IT (OUI) beauftragt, einen Pandemieplan für den **rbb** zu entwickeln. Auslöser war die sog. Schweinegrippe. Ziel des Planes war es, nicht nur das Verhalten anlässlich der Schweinegrippe, sondern generell zu regeln, wie der **rbb** auf Pandemien reagiert. OUI hatte dazu eine Arbeitsgruppe „AG Pandemie" initiiert. Vertreten waren neben Vertretern aller Direktionen, auch die Betriebsärztin, der Arbeitssicherheitsausschuss, der Personalrat und die Schwerbehindertenvertretung. Ich habe punktuell an der Erstellung des Plans mitgewirkt und mich dabei insbesondere zur Frage der Auskunftspflichten der Arbeitnehmer geäußert. Grundsätzlich stellt eine Verpflichtung des Arbeitnehmers, den Arbeitgeber über das Auftreten von Krankheitssymptomen oder Diagnosen zu informieren einen unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) dar. Etwas anderes gilt allerdings bei dem Verdacht einer ansteckenden Krankheit: In dieser Situation trifft den Arbeitnehmer eine Offenbarungspflicht, weil die gewichtigen Interessen des Arbeitgebers an einer Aufrechterhaltung des Betriebsablaufs sowie der übrigen Belegschaft an der Vermeidung einer Ansteckung insoweit überwiegen. In akuten Verdachtsfällen kann der Arbeitgeber auch darauf bestehen, dass sich der Arbeitnehmer einer ärztlichen Untersuchung unterzieht. In einer akuten Pandemiesituation ist sogar die Weisung des Arbeitgebers zulässig, die die Arbeitnehmer dazu verpflichtet, bei ihren Kollegen auftretende Grippesymptome anzuzeigen. Hier überwiegen ebenfalls das Interesse der noch gesunden Arbeitnehmer vor einer Infizierung geschützt zu werden, sowie die Pflicht des Arbeitgebers zur Gesundheitsvorsorge, denn nach § 2 Abs. 1 Arbeitsschutzgesetz hat der Arbeitgeber seine Arbeitnehmer während ihrer Arbeitstätigkeit vor Infek-

tionskrankheiten zu schützen, die besonders leicht übertragbar und/oder gefährlich sind.

Ende 2009 hat die Geschäftsleitung den von der AG Pandemie vorgelegten Pandemieplan beschlossen.

2. Dienstanweisung für die Führung und Verwaltung von Personalakten

Die Geschäftsordnung des Rundfunk Berlin-Brandenburg regelt in § 14 Abs. 3 Satz 3: „Näheres über die Führung und Aufbewahrung von sowie die Einsichtnahme in Personalakten regelt eine Dienstanweisung."

Auf dieser Grundlage hat die Personalabteilung in enger Abstimmung mit mir und dem Personalrat eine Dienstanweisung für die Führung und Verwaltung von Personalakten entworfen.

Die Dienstanweisung regelt in Ergänzung zu den tarifvertraglichen Regelungen und der Dienstanweisung für die Bearbeitung und Verwaltung von Dokumenten und Akten die Führung und Verwaltung von Personalakten und die Rechte der Arbeitnehmerinnen und Arbeitnehmer. Dazu gehören u.a. das Akteneinsichtsrecht, das Recht zur Stellungnahme vor nachteiligen Eintragungen und der Berichtigungsanspruch.

Dabei sind die datenschutzrechtlichen Aspekte selbstverständlich berücksichtigt worden.

3. Blutproben vor der Einstellung?

Im Herbst 2009 hatte der NDR in seinem Fernsehprogramm über Bluttests im Rahmen von Einstellungsuntersuchungen bei dem Autokonzern Daimler berichtet. Wie sich später herausstellte, hatte der NDR seinerzeit selbst Bluttest vor Einstellungen durchgeführt. Auch beim **rbb** – wie auch bei den meisten anderen Rundfunkanstalten – gehörten ursprünglich bei verpflichtenden

Einstellungsuntersuchungen für Mitarbeiterinnen und Mitarbeiter, die in eine unbefristete Festanstellung übernommen werden sollten, Bluttests zum Untersuchungsprogramm des externen Personalarztes. Der **rbb** erfuhr jedoch keinerlei Ergebnis des Tests, sondern nur das Endergebnis der Untersuchung, also die Zusammenschau aller Ergebnisse in Form eines „geeignet" bzw. „nicht geeignet". Inzwischen haben sich die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio intensiv mit der Thematik befasst und empfohlen, von Bluttests grundsätzlich abzusehen. Für den **rbb** war der Zeitpunkt günstig: Zum Jahreswechsel 2009/2010 fand ein Wechsel des externen Personalarztes statt. In Gesprächen mit dem neuen Vertragspartner, an denen ich teilgenommen habe, wurde vereinbart, dass der Umfang der einzelnen Untersuchungen arbeitsplatzorientiert und in Absprache mit der Personalabteilung erfolgen soll. In Abstimmung mit mir hat die Personalabteilung inzwischen ein Konzept für Einstellungsuntersuchungen erarbeitet. Es sieht lediglich für Tätigkeiten im Ausland noch Blutuntersuchungen vor, wobei ein Aids-Test und Genanalysen ausdrücklich ausgeschlossen sind.

4. Online-Buchungen bei der Deutschen Bahn

Die Verhandlungen mit der Deutschen Bahn über die Einführung eines Online-Buchungssystems, über die ich schon in meinem letzten Tätigkeitsbericht informiert habe, dauern weiter an.

Am 08. 03. 2010 hat ein Key Account Manager der DB Bahn dem Leiter der Abteilung Beschaffung, dem IT-Sicherheitsbeauftragten und mir das mögliche Verfahren vorgestellt. Danach ist es inzwischen für die Reisenden nicht mehr zwingend notwendig, sich gegenüber den Mitarbeitern der DB mit einer Kreditkarte auszuweisen. Es reichen Personalausweis oder Bahnkarte. Nachdem die Wirtschaftlichkeitsprüfung im **rbb** inzwischen abgeschlossen ist, erfolgt derzeit eine technische Prüfung des von der DB zur Verfügung gestellten Systems durch den IT-Sicherheitsbeauftragten. Im Anschluss daran sollen in Abstimmung mit mir die Verfahrensabläufe geplant werden.

5. Strukturuntersuchung Produktions- und Betriebsdirektion

Im Zuge der Strukturuntersuchung der Produktions- und Betriebsdirektion ist im Sommer 2009 eine Untersuchung des Produktionsaufwands in der Grafik hinsichtlich einzelner Sendungen des **rbb**-Fernsehprogramms initiiert worden. Zu diesem Zweck fand über einen längeren Zeitraum eine Aufwandserfassung über ein Tool in Lotus Notes statt, der ich zugestimmt hatte.

Die Aufwandserfassung erfolgte ausschließlich auf den Arbeitsplatz bezogen. In diesem Rahmen wurden die Tätigkeiten an allen 9 Workstations in Berlin und Potsdam, der Trickkamera und der Schriftgeräte erfasst. Es wurde dokumentiert, welche grafischen Aufgaben an den einzelnen Arbeitsgeräten unabhängig von den jeweiligen Mitarbeiterinnen und Mitarbeitern an welchem Tag und innerhalb welchen Zeitraums ausgeführt wurden. Außerdem wurde die Redaktion bzw. die Sendung erfragt, für die die Arbeit geleistet wurde. Betroffen waren alle freien und fest angestellten Mitarbeiterinnen und Mitarbeiter des Bereichs Grafik. Die Daten wurden monatlich durch die Leiterin der Abteilung Bild und den Projektverantwortlichen als Zugriffsberechtigte ausgewertet und anschließend gelöscht. Hierbei ging es darum, die Vielfalt der Arbeitsaufträge und den dazu nötigen Aufwand zu ermitteln. Die Ergebnisse der monatlichen Auswertung wurden mit dem Leiter der HA Produktion, dem Betriebs- und Produktionsdirektor und der Programmdirektorin besprochen.

6. Interne Leistungsverrechnung

Auch über das Vorhaben einer Internen Leistungsverrechnung habe ich in meinem letzten Tätigkeitsbericht bereits informiert. Die Gespräche zwischen Projektleitung und Personalrat u. a. zu Fragen der Datenerhebung und –auswertung, an denen ich beteiligt bin, dauern weiter an.

7. Einverständniserklärung in die Einholung von Auskünften zu polizeilichen Erkenntnissen

a) Jüdische Einrichtungen

Schon Ende 2008 hat mich der Personalrat darüber informiert, dass im Rahmen von Dreharbeiten in der Jüdischen Gemeinde zu Berlin und in anderen Jüdischen Einrichtungen wie z. B. dem Jüdischen Museum den technischen Mitarbeitern des **rbb** seit einiger Zeit ein Formular für eine Einverständniserklärung zur Durchführung einer allgemeinen Sicherheitsüberprüfung zur Unterschrift übersandt wird. Darin sollen sich die Betroffenen damit einverstanden erklären, dass die Einrichtung zum Zwecke einer allgemeinen Zuverlässigkeitsüberprüfung eine Anfrage beim Polizeipräsidenten in Berlin stellt. Die Einwilligung soll sich auf folgende polizeiliche Dateien und Datensammlungen beziehen: Landesdatensystem POLIKS, INPOL, INPOL neu und Dateien des Polizeilichen Staatsschutzes Berlin. Gegenüber der Jüdischen Gemeinde zu Berlin und gegenüber den Verantwortlichen im Jüdischen Museum habe ich in einem Schreiben zunächst meine Zweifel daran geäußert, dass es datenschutzrechtlich zulässig ist, eine derart weitreichende Einverständniserklärung von den **rbb**-Kollegen abzuverlangen. Die Verantwortlichen in den Jüdischen Einrichtungen haben mir gegenüber diese Praxis bestätigt und darauf verwiesen, dass dies eine Vorgabe des LKA sei. Vom Direktor des LKA erhielt ich auf Nachfrage im Juni 2009 ein Schreiben, in dem mir folgendes erläutert wurde: Das Verfahren wurde zwischen den Jüdischen Einrichtungen, der Senatsverwaltung für Inneres und Sport und dem Polizeipräsidenten in Berlin vereinbart und wird so seit 2006 angewendet. Um den **rbb**-Mitarbeitern wie den anderen Mitarbeitern von Fremdfirmen einen Zugang gewährleisten zu können, wird den betroffenen Personen die Einverständniserklärung zur Zuverlässigkeitsüberprüfung gem. § 44 Abs. 8 des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin i. V. m. §§ 12 Abs. 1, Satz 1, 11 Abs. 2 Satz 1, 6 Abs. 1 Satz 1 Nr. 3 Berliner Datenschutzgesetz ausgehändigt, die vom Betroffenen unterzeichnet werden muss, da sonst keine Überprüfung in den dort ebenfalls benannten Datensammlungen durchgeführt wird und vom LKA aus auch kein Bescheid ergehen kann. Weiterhin wird dem zu Überprüfenden mitgeteilt, dass nicht die über ihn gegebenenfalls vorhandenen Erkenntnisse, sondern nur die Tatsache, dass Erkenntnisse vorhanden sind, der Einrichtung als Antwort übermittelt wird. Die Einrichtung entscheidet dann beim Vorliegen von polizeilichen Er-

kenntnissen nach eigenem Ermessen über die Zusage bzw. Versagung einer Tätigkeit der Person in den sicherheitsrelevanten Bereichen. Der Antragsteller selbst wird unabhängig von der Mitteilung an die Jüdische Einrichtung bei einem Vorliegen von polizeilichen Erkenntnissen durch Schreiben an seine Melde-/Wohnanschrift benachrichtigt. Er wird belehrt, dass es ihr/ihm frei steht, nunmehr auch eine Selbstauskunft gemäß § 50 Abs. 1 ASOG Berlin zu beantragen. Als Ergebnis dieser Auskunft werden die gesammelten Erkenntnisse zur Person aufgelistet und mitgeteilt, gegebenenfalls wird auf eine Bitte um Datenlöschungen unter Berücksichtigung von amtlichen Prüffristen eingegangen. Diese Daten werden immer nur dem Antragsteller übermittelt. Bei Hinweisen zu Informationen in Dateien anderer deutscher Polizeien ergeht der schriftliche Hinweis auf Auskunft gem. § 19 Bundesdatenschutzgesetz durch das Bundeskriminalamt Wiesbaden. Die übermittelten Anfragen werden zwei Jahre als Tätigkeitsnachweis zur Zuverlässigkeitsprüfung elektronisch gespeichert.

Diese Auskunft hat mich überzeugt. Ich halte dieses Verfahren für datenschutzrechtlich korrekt. Dies habe ich auch gegenüber dem Personalrat zum Ausdruck gebracht.

b) Leichtathletik-Weltmeisterschaft

Im Vorfeld der Leichtathletik-Weltmeisterschaft 2009 in Berlin sind die Journalisten wie die Beschäftigten privater Sicherheitsdienste und Caterer sowie die freiwilligen Helferinnen und Helfer, die zum sicherheitsempfindlichen Bereich Zugang erhalten wollten, vom LKA auf ihre Zuverlässigkeit überprüft worden. Diese Überprüfungen haben zu heftigen Diskussionen geführt, nachdem Journalisten der „taz“ ihr Einverständnis dazu verweigert hatten.

Eine Rückfrage bei den betroffenen Kollegen im **rbb** hatte Anfang 2009 ergeben, dass die Anforderungen für eine Akkreditierung bei wichtigen Sportveranstaltungen als vertretbar empfunden und insbesondere auch deshalb akzeptiert werden, weil sie u.a. auch ihrer eigenen Sicherheit dienen. Aus diesem Grund habe ich davon abgesehen, die entsprechende Praxis in Frage zu stellen.

Die Rundfunkdatenschutzbeauftragten von ARD, ZDF und DLR haben verabredet, sich mit diesem Thema noch einmal grundsätzlich zu beschäftigen.

IV. Informationsmaßnahmen

Am 14.08.2009 habe ich zusammen mit dem IT-Sicherheitsbeauftragten das jährliche Datenschutzseminar für Azubis durchgeführt.

D. Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung

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 2009 rund 39,5 Millionen Teilnehmerkonten mit insgesamt angemeldeten rund 42, 9 Millionen Hörfunk- und 36, 7 Mio. Fernsehgeräten (davon gebührenpflichtig 39,1 Mio. Hörfunk- und 33,2 Mio. Fernsehgeräte, gebührenbefreit 3,8 Mio. Hörfunk- und 3,5 Mio. Fernsehgeräte).

Für den **rbb** stellen sich die Zahlen per 31.12.2009 wie folgt dar:
2.832.134 Teilnehmerkonten, 2.958.069 Hörfunkgeräte (davon befreit 395.537), 2.657.112 Fernsehgeräte (davon befreit 397.841).

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 Verstöße 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 2009 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	05
Fragen bzgl. der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung	10
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen	16
Verlangen, Teilnehmerdaten nicht zu anderen Zwecken zu nutzen bzw. zu übermitteln	01
Anfragen von Finanzämtern nach Daten (insbes. Bankverbindungen) von Rundfunkteilnehmern	00
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von	

Rundfunkteilnehmern	01
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz	07
Sonstige Anfragen im Zusammenhang mit der im Jahr 2009 durchgeführten Lastschriftzahler-Bestands-Pflegeaktion	10

Anzahl der Vorgänge insgesamt:	**50**

Ich selbst habe in 2009 folgende Vorgänge bearbeitet:

Beschwerden über die Vorgehensweise eines Rundfunkgebührenbeauftragten	01
Fragen im Zusammenhang mit der Glaubhaftmachung der Befreiungsvoraussetzungen	03
Fragen im Zusammenhang mit der Glaubhaftmachung des Grundes der Abmeldung	01
Fragen zum Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung bei nichteehelicher Lebensgemeinschaft (dazu s. u.)	03
Fragen bzgl. der Herkunft von Daten	03
Beschwerde wg. fehlerhafter Bearbeitung einer Anmeldung über das Internet-Portal der GEZ	01

Anzahl der Vorgänge insgesamt:	**12**

Im Vergleich zum Vorjahr (insgesamt 88 Anfragen und Beschwerden aus dem Sendegebiet des **rbb**) ist für das Jahr 2009 (62) ein beachtlicher Rückgang zu verzeichnen.

Den Anfragen zum Datenschutz bei nichtehelichen Lebensgemeinschaften lag jeweils folgender Sachverhalt zugrunde:

Rundfunkteilnehmerinnen hatten versucht, sich mit der Begründung von der Gebührenpflicht abzumelden, sie zögen zu ihrem Freund in dessen Haushalt und

dieser würde für die dort vorhandenen Rundfunkempfangsgeräte bereits Rundfunkgebühren zahlen. Mit Verweis auf Datenschutz verrieten sie der GEZ allerdings weder den Namen noch die Rundfunkteilnehmernummer des Partners, so dass die GEZ nicht nachprüfen konnte, ob für die Geräte im zukünftigen gemeinsamen Haushalt tatsächlich schon Rundfunkgebühren gezahlt würden. In der Konsequenz erkannte die GEZ die Abmeldungen nicht an.

Ich habe den Petentinnen mitgeteilt, dass ich die Vorgehensweise der GEZ für rechtlich zutreffend halte. Dies ergibt sich aus Folgendem:

Nach § 4 Abs. 1 RGebStV beginnt die Rundfunkgebührenpflicht mit dem ersten Tag des Monats, in dem ein Rundfunkempfangsgerät zum Empfang bereit gehalten wird. Ein Rundfunkgerät wird gemäß § 1 Abs. 2 Satz 2 RGebStV zum Empfang bereitgehalten, wenn damit ohne besonderen zusätzlichen technischen Aufwand Rundfunkdarbietungen, unabhängig von Art, Umfang und Anzahl der empfangbaren Programme, unverschlüsselt oder verschlüsselt empfangen werden können. Nach dem eindeutigen Wortlaut dieser Vorschriften entsteht die Gebührenpflicht, wenn und sobald ein Rundfunkempfangsgerät tatsächlich zum Empfang bereit gehalten wird. Mehrere Personen können Rundfunkempfangsgeräte auch gemeinsam zum Empfang bereithalten. Sie haften in diesem Fall als Gesamtschuldner gemäß § 421 BGB für die zu entrichtenden Rundfunkgebühren. Die Rundfunkanstalt kann die anfallenden Rundfunkgebühren von jedem Gesamtschuldner nach Belieben fordern, hat jedoch insgesamt nur einmal Anspruch darauf. Nichteheliche Lebenspartner halten Rundfunkempfangsgeräte innerhalb einer Wohnung regelmäßig gemeinsam zum Empfang bereit. Nach § 7 Abs. 3 Satz 1 RGebStV sind die Rundfunkgebühren als Schickschuld zu entrichten, d. h. die Rundfunkgebühren sind auf Kosten und Gefahr des Rundfunkteilnehmers zu übermitteln. Daraus folgt, dass die Rundfunkteilnehmerin die Beweislast für die Erfüllung ihrer Schuld trägt. Sie ist insoweit gegenüber der GEZ auch nach § 4 Abs. 5 RGebStV auskunftspflichtig, weil Grund und Höhe ihrer eigenen Gebührenpflicht durch Zahlungen ihres Lebensgefährten betroffen werden. Solange die Rundfunkteilnehmerin nicht nachweist, dass ihr Lebensgefährte die Rundfunkgebühren zahlt, ist sie ihrerseits weiterhin gebührenpflichtig.

III. GEORG

Die Gebühreneinzugsordnung (GEORG) regelt für die GEZ und die Rundfunkanstalten die Verfahrensgrundsätze des Rundfunkgebühreneinzugsverfahrens und der damit verbundenen Aufgaben. Aufbauend auf den rundfunkrechtlichen Normen (insbesondere Rundfunkgebührenstaatsvertrag, Rundfunkfinanzierungsstaatsvertrag und Satzungen der Landesrundfunkanstalten über das Verfahren zur Leistung der Rundfunkgebühren) enthält GEORG eine allgemeine Beschreibung der Grundsätze des Gebühreneinzugsverfahrens und bildet den Rahmen für weitere Detailregelungen (insbesondere EDV-Programme, Organisationshandbücher und Arbeitsanweisungen).

Durch die Einführung eines Managementsystems für Informationssicherheit in der GEZ und der geplanten Zertifizierung nach der ISO 7001 wurden neben zahlreichen Maßnahmen auch in der GEORG einige Anpassungen, insbesondere bei den Regelungen zur IT-Sicherheit, notwendig. Dadurch ist dokumentiert, dass vergleichbar hohe IT-Sicherheitsstandards wie bei der GEZ auch in allen Rundfunkanstalten vorhanden sind. Die Anpassung der GEORG ist im Frühjahr 2010 mit den Rundfunkdatenschutzbeauftragten abgestimmt worden. Die GEZ-Zertifizierung ist für Oktober 2010 geplant.

IV. Mobile Datenabfragegeräte für die Rundfunkgebührenbeauftragten

In meinem letzten Tätigkeitsbericht hatte ich darüber informiert, dass der **rbb** – wie auch alle anderen Landesrundfunkanstalten – seinen Rundfunkgebührenbeauftragten neuerdings die Möglichkeit einräumt, mit mobilen Datenabfragegeräten über eine Mobilfunkverbindung auf einen eingeschränkten Datensatz der GEZ-Teilnehmerbank zuzugreifen, um damit in der Lage zu sein, Fragen zum Teilnehmerstatus vor Ort klären zu können. Der Einsatz der Blackberrys erfolgt auf freiwilliger Basis.

Wie angekündigt, wurde das von mir mit dem IT-Sicherheitsbeauftragten erarbeitete Datensicherheitskonzept inzwischen mit den für den **rbb** zuständigen Landes-

datenschutzbeauftragten von Berlin und Brandenburg abgestimmt. Das Konzept sieht u. a. Folgendes vor: Ausschließlich den langjährigen Hauptbeauftragten wird eine überregionale Zugriffsmöglichkeit auf das GEZ-Teilnehmerdatensystem eingeräumt. Die sog. Unterbeauftragten erhalten lediglich eine beschränkte Zugriffsmöglichkeit auf die Region Berlin/Brandenburg. Bei neu ermächtigten Unterbeauftragten wird der **rbb** frühestens nach drei Monaten erfolgreicher Tätigkeit einen Zugang zu dem System gewähren. Damit besteht genügend Zeit, die Seriosität und Arbeitsweise der Unterbeauftragten zu prüfen. Die mobilen Geräte bleiben im Eigentum des **rbb.** Durch eine entsprechende Konfiguration ist sichergestellt, dass die Nutzer die Geräte ausschließlich zur Erfüllung ihrer Aufgaben als Rundfunkgebührenbeauftragte nutzen können. In speziellen vertraglichen Regelungen werden den Nutzern Vorgaben zum Gebrauch der Geräte gemacht. Nach Einweisung durch den Abteilungsleiter Rundfunkgebühren, den IT-Sicherheitsbeauftragten und mich im Januar 2010 wurden inzwischen insgesamt 15 Blackberrys ausgegeben. Die Handhabung der kleinen Geräte erfordert eine gewisse Übung. Ferner beklagen die Nutzer lange Antwortzeiten bis zur Meldung aus dem GEZ-System. Aus diesen Gründen ist die Zahl der Anwender bislang auf kleinem Niveau. Derzeit werden Möglichkeiten der Verbesserungen geprüft.

V. Datenschutz bei der Fa. Creditreform

Im Auftrag der GEZ bzw. der Landesrundfunkanstalten führt die Fa. Creditreform in Mainz das Inkasso von Rundfunkgebührenforderungen durch, die durch die Finanzämter nicht vollstreckt werden konnten. Pro Jahr können auf diese Weise für den **rbb** mehrere Hunderttausend Euro zusätzlich realisiert werden. 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. In der Folge hat der Rundfunkdatenschutzbeauftragte des SWR einen Entwurf für eine Vertragsergänzung erarbeitet, die die Vorgaben der Rundfunkanstalten zu Datenschutz und Datensicherheit verschärft. Derzeit finden dazu noch Abstimmungen mit den zuständigen Landesdatenschutzbeauftragten statt.

E. Datenschutz im Informationsverarbeitungszentrum (IVZ)

Beim **rbb** wird als Gemeinschaftseinrichtung von MDR, NDR, RB, Deutschlandradio, **rbb** und SR das rechtlich unselbstständige Informationsverarbeitungszentrum 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 15.09.2010 fand beim IVZ das jährliche Treffen der Datenschutzbeauftragten der beteiligten Anstalten und des IVZ statt. Es wurde über das BSI-Re-Zertifizierungsverfahren und einige weitere datenschutzrechtlich relevante Projekte des IVZ berichtet.

F. Datenschutz im ARD-Hauptstadtstudio (HSB)

Wie schon in meinem Vorjahresbericht erwähnt, muss das ARD-Hauptstadtstudio seine Telekommunikationsanlage-Anlage erneuern. Die Anlage versorgt neben ca. 350 herkömmlichen Telefonanschlüssen auch weitere rund 250 Anschlüsse für die Hörfunk-Audioübertragung aller neun im Haus arbeitenden ARD-Anstalten (Audio-Codecs).
Notwendig geworden ist diese Maßnahme, da der Hersteller der ursprünglichen Anlage sowohl den Support als auch die Ersatzteilversorgung gekündigt hat. Das neue Telekommunikationssystem ist eine reine Voice-Over-IP-Anlage (Telefon über IT-Strukturen). So verschmilzt die herkömmliche Telefonie mit der modernen IT-Welt.

Zusammen mit dem IT-Sicherheitsbeauftragten und einer Vertreterin des Personalrats bin ich seit September 2009 in die Projektplanung einbezogen. Bei den Festlegungen zur Konfiguration der Telefonanlage ging es mir insbesondere um die Wahrung des Telekommunikationsgeheimnisses der Mitarbeiter im ARD-HSB und um die Sicherstellung des Informantenschutzes. Eine Besonderheit bestand darin, dass die Errechnung der privaten Telefonkosten der Mitarbeiter des HSB zukünftig mit Hilfe einer speziellen Software beim **rbb** vorgenommen wird. Die ermittelten Kosten werden der Verwaltungsleiterin im HSB mitgeteilt, die diese an die jeweils entsendenden Rundfunkanstalten weiterleitet, da die Telefonkosten vom Gehalt der Mitarbeiterinnen und Mitarbeiter des HSB abgezogen werden. Durch entsprechende Verfahrensregelungen wird die Datenverarbeitung auch bei diesem Bereich auf das erforderliche Minimum reduziert.

Im Frühjahr dieses Jahres hat der Probebetrieb der Telefonanlage begonnen. Die Verhandlungen über die Anpassung der Dienstvereinbarung werden demnächst abgeschlossen sein.

G. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) hat im Berichtszeitraum unter meinem Vorsitz zweimal getagt: am 27./28. April 2009 beim Bayerischen Rundfunk in München und am 01./02. Oktober 2009 in Erfurt beim Kinderkanal. Außerdem hat eine Telefonschaltkonferenz am 13. August 2009 stattgefunden.

Auf der Sitzung in München haben wir uns ausführlich mit den datenschutzrechtlichen Aspekten bei den interaktiven TV-Angeboten im Programmbouquet ARD Digital beschäftigt. Zu diesem Tagesordnungspunkt erläuterte uns der Leiter des ARD Play-Out-Centers in Potsdam, Herr Hans-Joachim Voigt, die bisherigen Entwicklungen. Es fand eine ausführliche Präsentation und Demonstration zu den

interaktiven Begleitdiensten, die über das ARD Play-Out-Center verbreitet werden, insbesondere unter Einbindung des ARD-Portals mit dem elektronischen Programmführer statt. Mit sog. Hybrid-Set-Top-Boxen kann zukünftig die Möglichkeit genutzt werden, Zusatzinformationen zum laufenden Bild über eine Internet-Verbindung zu laden. Mit dieser Technik ist es z. B. auch möglich, über die Suchfunktion personalisierte Programmempfehlungen zu geben und (interessant für kommerzielle Sender) personalisierte Werbebotschaften zu versenden. Durch die Internet-Verbindung entsteht ein echter Rückkanal. Über die IP-Adresse ist der Nutzer personalisierbar. Der AK DSB hat seine Forderung bekräftigt, die Möglichkeit des anonymen Fernsehens auch in Zukunft zu erhalten. Mit Herrn Voigt wurde verabredet, dass er uns über weitere datenschutzrelevante Entwicklungen auf dem Laufenden hält.

Ein weiterer Schwerpunkt unserer Beratungen waren Datenschutz und Datensicherheit bei der Fa. Creditreform in Mainz, die für die Rundfunkanstalten Rundfunkgebührenforderungen eintreibt, sowie Fragen des Datenschutzes und der Datensicherheit bei der Beihilfe- und Bezüge-Zentrum GmbH in Bad Dürkheim, die für einige der Rundfunkanstalten (u. a. für den **rbb**) die Beihilfeanträge der Mitarbeiterinnen und Mitarbeiter bearbeitet. In beiden Fällen handelt es sich um Auftragsdatenverarbeitung. Da beide Institutionen in Rheinland-Pfalz liegen, führt der Rundfunkdatenschutzbeauftragte der ortsansässigen Rundfunkanstalt SWR, Herr Prof. Herb, regelmäßig federführend Kontrollen vor Ort durch.

Weitere Themenschwerpunkte unserer Beratungen im AK DSB waren Fragen im Zusammenhang mit der Umstellung der Rundfunkfinanzierung auf das neue Rundfunkbeitragssystem und insbesondere mit der dafür erforderlichen einmaligen Datenübermittlung der Meldedaten an die Landesrundfunkanstalten zum Zwecke der Bestands- und Ersterfassung und die Auswirkungen der BDSG-Novellen insbesondere auf den Arbeitnehmerdatenschutz bei den Rundfunkanstalten und die Mailing-Maßnahmen der GEZ.

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 beratendes Mitglied habe ich auch im Berichtszeitraum den AK DSB in diesem Gremium vertreten. Das IT-Sicherheitsgremium hat im Berichtzeitraum am 07.10.2009 in Saarbrücken getagt. Dort ging es um das Anforderungsprofil an die sicherheitstechnische Untersuchung des ARD-Daten-CN, um Sicherheitsstandards für Web-Anwendungen im ARD-CN. Eine weitere Sitzung fand am 24.02.2010 beim MDR in Leipzig statt. Dort ging es u. a. um die Risiken beim Einsatz von Unified-Communication-Tools (wie beispielsweise „Skype“) in Rundfunknetzen.

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 mich mit dieser Aufgabe betraut. Im Berichtszeitraum fand eine Sitzung des AK Medien am 17. 09. 2009 in Potsdam statt. Themen waren u. a. Einzelheiten zum Gebührenbefreiungsverfahren, der 13. Rundfunkänderungsstaatsvertrag, und aktuelle Entwicklungen beim Cloud-Computing. An der Sitzung des AK Medien am 24./25. Februar 2010 in Berlin war ich aufgrund einer Terminkollision verhindert. Der Datenschutzbeauftragte des WDR hat mich vertreten.

Berlin, 09. September 2010

gez. Anke Naujock