

1. Tätigkeitsbericht

der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg

**Berichtszeitraum:
1. Mai 2003 bis 31. März 2004**

Dem Rundfunkrat vorgelegt von Anke Naujock

Vorbemerkung

Der Bundesdatenschutzbeauftragte Peter Schaar hat in einer kürzlich gehaltenen Rede davor gewarnt, dass sich die Datenschützer nicht in die Ecke der „Bedenkenträger“ abschieben lassen dürfen.

Darum, dass ich in dieser „Ecke“ nicht lande, bin ich von Anfang an bemüht gewesen.

Mir geht es darum, allen im RBB – der Geschäftsleitung und den Kolleginnen und Kollegen - zu vermitteln, dass sich Datenschutz und Datensicherheit lohnen. Wird der Datenschutz beachtet und in geeignete technische und organisatorische Maßnahmen zur IT-Sicherheit investiert (intellektuell und – dort, wo es im Einzelfall erforderlich ist - auch materiell) , werden nicht nur die Risiken für die Vertraulichkeit, Verfügbarkeit und Korrektheit der Daten verringert. Als Nebeneffekt wird in der Regel ein insgesamt reibungsloserer Verfahrensablauf erzielt. Außerdem steigt die Akzeptanz der Mitarbeiterinnen und Mitarbeiter für den Einsatz neuer Techniken.

Zwar komme auch ich nicht umhin, im Einzelfall auf Gefahren für den Datenschutz hinzuweisen und immer wieder an die Einhaltung datenschutzrechtlicher Bestimmungen zu erinnern. Den Schwerpunkt meiner Arbeit bilden jedoch die sog. Vorabkontrollen, die ich gemäß den Vorgaben des Berliner Datenschutzgesetzes jeweils vor der Einführung neuer technischer Systeme, mit denen personenbezogene Daten verarbeitet werden, durchführe. Zusammen mit den Projektverantwortlichen erarbeite ich jeweils Lösungen, die dem Datenschutz Rechnung tragen. Dabei werde ich in der Regel vom IT-Sicherheitsbeauftragten unterstützt, dessen Aufgabe es ist, die dafür erforderlichen Datensicherheitskonzepte zu erarbeiten.

Herrn Eberhard Mohr, der die Ämter des IT-Sicherheitsbeauftragten und des stellvertretenden behördlichen Datenschutzbeauftragten im Berichtszeitraum kommissarisch wahrgenommen hat, möchte ich an dieser Stelle für seine Unterstützung herzlich danken.

Bei der Intendantin, den weiteren Mitgliedern der Geschäftsleitung und den sonstigen Verantwortungsträgern möchte ich mich für das mir entgegengebrachte Vertrauen bedanken. Meine Anregungen zur Verbesserung von Datenschutz und Datensicherheit wurden stets aufgegriffen und deren Umsetzung veranlasst. Dem Personalrat danke ich für die vertrauensvolle Zusammenarbeit.

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

I. Staatsvertragliche Regelung

1. Rundfunkdatenschutzbeauftragte gemäß RBB-Staatsvertrag

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

Die Aufgaben des/der Rundfunkdatenschutzbeauftragten sind in § 38 Abs. 2 bis 7 geregelt. Gemäß Abs. 2 Satz 2 überwacht er/sie die Einhaltung der Datenschutzvorschriften des RBB-Staatsvertrages 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 Rundfunk Berlin-Brandenburg dem Landesbeauftragten für den Datenschutz des Landes Berlin. Die Kontrolle erfolgt im Benehmen mit dem Landesbeauftragten des Datenschutzes des anderen Landes (Abs. 8).

Die Datenschutzbeauftragte des RBB ist also – wie schon bei ORB und SFB und wie die Datenschutzbeauftragten des Hessischen Rundfunks und von Radio Bremen – nur für die Kontrolle der Datenverarbeitung im journalistisch-redaktionellen Bereich zuständig. Die Kontrolle der Datenverarbeitung im wirtschaftlich-administrativen Bereich obliegt hingegen den Landesdatenschutzbeauftragten.

Im Unterschied dazu haben die Rundfunkdatenschutzbeauftragten von SWR, BR, WDR, SR, NDR, MDR sowie des ZDF und des DLR eine umfassende Kontrollzuständigkeit in Bezug auf sämtliche Aktivitäten der Rundfunkanstalten.

Darauf, dass die teilweise Kontrollzuständigkeit der Landesdatenschutzbeauftragten für den öffentlich-rechtlichen Rundfunk zumindest verfassungsrechtlich bedenklich ist, haben die Justitiarinnen und Justitiare von ARD, ZDF und DLR immer wieder hingewiesen (so

auch Dörr „Rundfunk und Datenschutz – Die Stellung des Datenschutzbeauftragten“ 2002, 48 ff). Aus dem Gebot der Staatsferne leitet sich ein umfassendes Selbstverwaltungsrecht der öffentlich-rechtlichen Rundfunkanstalten ab. Damit ist eine Kontrolle des Datenschutzes durch externe staatliche Behörden nicht vereinbar.

Überdies zeigt die Praxis, dass eine Aufspaltung in den journalistisch-redaktionellen und wirtschaftlich-administrativen Bereich oftmals nicht möglich ist. Ein aktuelles Beispiel für diese Problematik habe ich unter E. II. beschrieben.

2. Behördliche Datenschutzbeauftragte gemäß § 19 a Berliner Datenschutzgesetz

Für die Sicherstellung des Datenschutzes im wirtschaftlich-administrativen Bereich ist beim RBB – wie bei allen Berliner Behörden und sonstigen öffentlichen Stellen - ein behördlicher/ eine behördliche Datenschutzbeauftragte und ein/e Stellvertreter/in zu bestellen (§ 36 Abs. 1 RBB-Staatsvertrag i.V. m. § 19 a Berliner Datenschutzgesetz – BlnDSG).

Die Funktionen des/der Rundfunkdatenschutzbeauftragten nach § 38 Abs. 1 RBB-Staatsvertrag und des/der behördlichen Datenschutzbeauftragten gemäß § 19 a BlnDSG werden wegen der in der Praxis häufig vorkommenden Abgrenzungsschwierigkeiten zwischen dem journalistisch-redaktionellen und dem wirtschaftlich-administrativen Bereich zweckmäßigerweise von ein und derselben Person wahrgenommen.

II. Konkrete Situation

Auf seiner Sitzung am 26. Mai 2003 hat mich der Rundfunkrat gemäß § 38 Abs. 1 RBB-Staatsvertrag auf Vorschlag der Intendantin für eine Amtszeit von vier Jahren zur Beauftragten für den Datenschutz des Rundfunk Berlin- Brandenburg bestellt.

Gemäß dem Beschluss der Geschäftsleitung vom 24. Juni 2003 hat mich die Intendantin für den gleichen Zeitraum auch mit der Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten im Sinne von § 19 a Berliner Datenschutzgesetz beauftragt. Die Funktion des stellvertretenden behördlichen Datenschutzbeauftragten nimmt zur Zeit Herr Eberhard Mohr kommissarisch wahr.

B. Entwicklung des Datenschutzrechts

I. Gesetze und Rechtsverordnungen

1. Neuordnung des Mediendatenschutzes

Der Schutz der personenbezogenen Daten der Nutzer von elektronischen Medien ist derzeit in verschiedenen – jedoch inhaltlich weitestgehend einheitlichen Regelwerken in Bund und Ländern geregelt. Für den Bereich der Tele- und Mediendienste wurden 1997 die spezifischen Datenschutzbestimmungen im geltenden Teledienstedatenschutzgesetz (TDDSG) des Bundes und im Mediendienste-Staatsvertrag (MDStV) der Länder geschaffen. Ebenso enthält der Rundfunkstaatsvertrag (RStV) der Länder vergleichbare Datenschutzbestimmungen für den Rundfunk. Der Datenschutz im öffentlich-rechtlichen Rundfunk ist in Sonderregelungen der einzelnen Landesdatenschutzgesetze bzw. in den jeweiligen Rundfunkgesetzen geregelt.

Der Telekommunikations (TK)-Datenschutz ist im Telekommunikationsgesetz und in der auf den dortigen Vorschriften beruhenden Telekommunikationsdatenschutz-Verordnung (TDSV) geregelt. Die Regelwerke zum IuK- und TK-Datenschutz stehen zumindest teilweise in einem Spannungsverhältnis zueinander, das bei den betroffenen Diensteanbietern zu erheblicher Rechtsunsicherheit führt.

Zukünftig soll der Datenschutz in den Tele- und Mediendiensten einheitlich durch den Bund geregelt werden. Hierzu soll ein neues Gesetz auf Bundesebene geschaffen werden, das auf den geltenden Bestimmungen in Bund und Ländern aufbaut und diese ersetzt. Für den Bereich des Rundfunkdatenschutzes, der als Annexkompetenz zum Rundfunk nur durch die Länder geregelt werden kann, besteht bei diesen die Überlegung, eine entsprechende Vereinheitlichung durch eine Verweisung im RStV auf dieses neue Bundesgesetz vorzunehmen.

Die Neuordnung des Datenschutzes in den elektronischen Medien ist ein erster Schritt im Zusammenhang mit dem Vorhaben einer groß angelegten Datenschutzreform, die das allgemeine Bundesdatenschutzgesetz (BDSG) und alle spezifischen Datenschutzvorschriften umfasst und das innerhalb eines größeren Zeithorizontes verwirklicht werden soll.

Die Ziele der Vereinheitlichung des Mediendatenschutzes und der Verbesserung der Transparenz der Datenschutzbestimmungen in diesem Bereich sind zu begrüßen. Die Vertreter des öffentlich-rechtlichen Rundfunks müssen den Neuordnungsprozess jedoch auch weiterhin kritisch begleiten und dabei darauf achten, dass seinem besonderen verfassungsrechtlichen Status im materiellen Datenschutzrecht und bei der Zuordnung der Kontrollkompetenzen Rechnung getragen wird.

2. Novellierung des Telekommunikationsgesetzes

Auf Initiative der Bundesregierung wird das Telekommunikationsgesetz (TKG) derzeit einer umfassenden Novellierung unterzogen. Damit sollen eine Reihe von europäischen Richtlinien – darunter die Richtlinie 2002/58/EG zum Datenschutz in der elektronischen Kommunikation - umgesetzt werden. Die entsprechende Anpassungsfrist wurde im Oktober 2003 bereits überschritten, so dass die Europäische Kommission inzwischen gegen die Bundesrepublik ein Vertragsverletzungsverfahren eingeleitet hat.

Der Schwerpunkt des Gesetzgebungsverfahrens liegt zwar bei der Neuordnung der Marktregulierung. Jedoch sind auch die datenschutzrechtlichen Bestimmungen von den geplanten Änderungen betroffen.

Um den gesamten Telekommunikationsdatenschutz zu straffen und um Redundanzen zu vermeiden, ist beabsichtigt, die Vorschriften der Telekommunikations-Datenschutzverordnung (TDSV) in das TKG zu übernehmen.

Geplant ist u. a. eine Rechtsgrundlage zur Erhebung von Kundendaten im Zusammenhang mit der Bereitstellung von TK-Dienstleistungen, die im voraus bezahlt werden (sog. Prepaid-Produkte). Die Kundendaten sind für die Abwicklung des Vertrages nicht erforderlich und dienen ausschließlich den Interessen der Strafverfolgungs- und Sicherheitsbehörden.

Diese Datenvorratsspeicherung bei Prepaid-Produkten ist aus allgemeinen datenschutzrechtlichen Erwägungen abzulehnen. Darüber hinaus erschwert sie die journalistische Arbeit unverhältnismäßig. Journalisten, die investigativ arbeiten, sind vielfach auf geschützte Kontaktaufnahme mit Informanten angewiesen. Durch die Registrierung der Prepaid-Handys wird ihnen ein Instrument zur Wahrung des Informantenschutzes und des Redaktionsgeheimnisses vorenthalten.

Des Weiteren ist vorgesehen, den Kreis derjenigen, die nach dem TKG grundsätzlich zur Vorhaltung technischer Einrichtungen für die Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation verpflichtet werden („Betreiber von Telekommunikationsanlagen“), beizubehalten. Die gebotene Eingrenzung dieses Kreises, insbesondere auf die Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden, soll wie bisher in der Telekommunikations-Überwachungsverordnung (TKÜV) erfolgen.

Es gibt keinen nachvollziehbaren Grund, warum eine Begrenzung des Kreises der Betroffenen erst in der Rechtsverordnung geschehen soll. Eine Einschränkung im Gesetz wäre schon aus Gründen der Rechtsklarheit sachgerecht.

Die Datenschutzbeauftragten von ARD, ZDF und DLR haben auf eine eigene Stellungnahme zum Gesetzentwurf der Bundesregierung verzichtet, ihre Positionen jedoch in die allgemeine Stellungnahme von ARD, ZDF und DLR eingebracht. Es bleibt abzuwarten, inwieweit sie bei dem Gesetzesvorhaben Berücksichtigung finden.

3. Strafprozessordnung (StPO)

Das Bundesministerium der Justiz (BMJ) hatte im September 2002 eine Veröffentlichung vorgelegt, die das Ergebnis des von ihm in Auftrag gegebenen Forschungsprojektes „Informationserhebung und -verwertung durch Vernehmung, Auskunft und heimliche Ermittlungsmaßnahmen“ enthält. In der Veröffentlichung wird eine Änderung der Strafprozessordnung (StPO) angeregt, die eine Stärkung der Zeugnisverweigerungsrechte in den Fällen des § 53 Abs. 1 Satz 1 Nr. 2, 4 und 5 StPO im Hinblick auf die Telekommunikationsüberwachung und andere heimliche Ermittlungsmaßnahmen zum Gegenstand haben.

Betroffen ist § 100 a StPO (Überwachung der Telekommunikationsinhalte), der dem Schutz der beruflichen Kommunikation von Journalisten keine Rechnung trägt. Die Regelung des § 100 a StPO führt mit ihren Möglichkeiten, die Telekommunikation unverdächtiger Zeugnisverweigerungsberechtigter zu überwachen, zu einer Verletzung des grundgesetzlich geschützten Redaktionsgeheimnisses und des Informantenschutzes.

Weiterhin sind §§ 100 g, 100 h und 100 i StPO (Überwachung von Telekommunikationsvorgängen) betroffen. Nach §§ 100 g und 100 h StPO müssen Telekommunikationsunternehmen Verbindungsdaten gemäß § 100 g StPO preisgeben, wenn Personen einer Straftat von „erheblicher Bedeutung“ gemäß § 100 a StPO oder einer Straftat verdächtigt werden, die mittels einer Endeinrichtung (z. B. Telefon, Satellitenfunkanlagen oder PC) begangen wird und Gründe der Verhältnismäßigkeit nicht entgegenstehen.

In § 100 h Abs. 2 StPO wird geregelt, dass das Zeugnisverweigerungsrecht für Geistliche, Verteidiger oder Abgeordnete dem Verlangen einer Auskunft über Telekommunikationsverbindungen, die von dem oder zu dem Zeugnisverweigerungsberechtigten hergestellt wurden, vorgeht. Insoweit ist das Verlangen unzulässig. Für zeugnisverweigerungsberechtigte Journalisten gilt diese Ausnahme von der Telekommunikationsüberwachung nicht.

Gemeinsam mit den Medienverbänden und -unternehmen DJV, BDZV, Deutscher Presserat, ver.di, VDZ, VPRT und ZDF hat die ARD eine Stellungnahme gegenüber dem BMJ zu dem aus dem genannten Forschungsprojekt hervorgegangenen Gesetzentwurf verfasst, der den konzeptionellen Ansatz verfolgt, die geltenden Regelungen der Strafprozessordnung zur Telekommunikationsüberwachung und dem Einsatz besonderer technischer Mittel im Interesse der Berufsgeheimnisträger (insbesondere Journalistinnen und Journalisten) zum Schutz berufsbezogener Kommunikation zu überarbeiten. Das Zeugnisverweigerungsrecht und das flankierende Beschlagnahmeverbot in § 53 und § 97 StPO schützen diese Kommunikationsvorgänge bisher nur unvollkommen. Der Schutz kann durch die Überwachung der Telekommunikation und weitere heimliche Ermittlungsmaßnahmen in erheblichem Umfang umgangen und eingeschränkt werden. Mit Hilfe der geltenden Vorschriften der §§ 100 a ff StPO ist es möglich, Informanten der Medien aufzuspüren und das Redaktionsgeheimnis zu durchbrechen. Es ist nach geltenden Vorschriften kein gesetzgeberisches Gesamtkonzept der Lösung des Problems erkennbar.

Zwar hat das Bundesverfassungsgericht mit Urteil vom 12. März 2003 in den Verfassungsbeschwerden des ZDF und einer Reporterin des Magazins „Stern“ keinen grundrechtsverletzenden Eingriff in Art. 5 Abs. 1 Satz 2 GG darin gesehen, dass auf Anordnung der Gerichte von Telekommunikationsunternehmen die Verbindungsdaten eines Handys des ZDF bzw. eines Handys und zweier Festnetzanschlüsse der Reporterin des „Stern“ herausgegeben werden mussten (BVerfG AfP 2003, 138).

Die Entscheidung des Bundesverfassungsgerichts bestätigt aber die Notwendigkeit, im Regelungsbereich heimlicher Ermittlungsmaßnahmen den Schutz der beruflichen Kommunikation von Journalisten zu stärken. Dabei geht es nicht darum, Journalisten allgemein und umfassend von Maßnahmen der Erhebung von Informationen über den Telekommunikationsverkehr bei der Aufklärung von Straftaten zu verschonen. Vielmehr muss es das Ziel gesetzgeberischer Maßnahmen sein, die Regelungen der §§ 53 Abs. 1 Nr. 5 und § 97 Abs. 5 StPO mit denen der Telekommunikationsüberwachung in Einklang zu bringen. Die Divergenz zwischen dem Recht des Journalisten, einerseits (aktiv) seine Informanten schützen und den Gewahrsam an Unterlagen aufrecht erhalten zu können, es andererseits aber (passiv) erdulden zu müssen, dass dieser Schutz durch Überwachungsmaßnahmen der Telekommunikation (und weiterer heimlicher Ermittlungsmaßnahmen) unterlaufen werden kann, muss beseitigt werden.

4. Bundesratsinitiative zum Schutz der Intimsphäre

Auf eine Bundesratsinitiative gehen die Bestrebungen zur Schaffung eines neuen Straftatbestands zum Schutz der Intimsphäre vor unbefugten Bildaufnahmen zurück.

Nach einem neuen § 201 a StGB soll mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft werden, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt. Ebenso soll bestraft werden, wer eine durch eine Tat nach Absatz 1 hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht und wer eine befugt hergestellte Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschütztem Raum befindet, unbefugt gebraucht oder einem Dritten zugänglich macht und dadurch deren höchstpersönliche Lebensbereich verletzt.

Damit soll der strafrechtlich nicht ausreichend gewährleistete Schutz der Intimsphäre vor Fällen, in denen Personen Kameraaugen an versteckter Stelle z.B. in Hotel- oder Gästezimmern, Toiletten oder Umkleidekabinen installieren, um in die Privat- oder Intimsphäre Dritter unbefugt einzudringen, nachgeholt werden.

Dieses Ziel ist auch aus datenschutzrechtlicher Sicht zu begrüßen. Würde allerdings das Gesetz in der derzeit vorliegenden Fassung in Kraft treten, wäre damit – sicherlich unge-

wollt – auch eine massive Einschränkung der Arbeit der Medien insbesondere auf den Gebieten des investigativen Journalismus und der Tatortberichterstattung verbunden.

Die Medienvertreter fordern daher gemeinsam zu Recht eine Überarbeitung des Entwurfs. Dabei müsste der Wortlaut im Interesse der Rechtssicherheit klarer gefasst werden. Außerdem sollte ein ausdrücklicher Rechtfertigungsgrund für die Arbeit der Medien aufgenommen werden.

II. Urteile

Entscheidung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung (sog. großer Lauschangriff)

Das Bundesverfassungsgericht hat mit Urteil vom 3. März 2004 – 1 BvR 2378/98 und 1 BvR 1084/99 – entschieden, dass ein erheblicher Teil der Vorschriften der Strafprozessordnung (StPO) zur Durchführung der akustischen Überwachung von Wohnraum zu Zwecken der Strafverfolgung verfassungswidrig ist. Der Gesetzgeber ist verpflichtet, einen verfassungsgemäßen Rechtszustand bis spätestens zum 30. Juni 2005 herzustellen. Bis zu diesem Termin können die beanstandeten Normen nach Maßgabe der Gründe weiterhin angewandt werden, wenn gesichert ist, dass bei der Durchführung der Überwachung der Schutz der Menschenwürde gewahrt und der Grundsatz der Verhältnismäßigkeit eingehalten wird.

Das BVerfG fordert in seiner Entscheidung eine restriktive, an der Menschenwürde orientierte Auslegung des Art. 13 Abs. 3 GG.

Die Unverletzlichkeit der Wohnung habe einen engen Bezug zur Menschenwürde und zu dem verfassungsrechtlichen Gebot unbedingter Achtung einer Sphäre der ausschließlich privaten – „höchstpersönlichen“ - Entfaltung. Die vertrauliche Kommunikation benötige einen räumlichen Schutz, auf den die Bürger vertrauen können. Dem Einzelnen soll das Recht „in Ruhe gelassen“ zu werden, gerade in seinen privaten Wohnräumen gesichert sein, und zwar ohne Angst, dass staatliche Stellen die Entfaltung seiner Persönlichkeit im Kernbereich privater Lebensgestaltung überwachen.

In diesen Kernbereich dürfe die akustische Überwachung von Wohnraum nicht eingreifen, und zwar auch nicht im Interesse der Effektivität der Strafrechtspflege und der Erforschung der Wahrheit. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung und dem Strafverfolgungsinteresse finde insoweit nicht statt. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diese Freiheit zur Entfaltung in den höchstpersönlichen Angelegenheiten nicht rechtfertigen.

Allerdings verletze nicht jede akustische Überwachung die Menschenwürde. So gehörten Gespräche über begangene Straftaten ihrem Inhalt nach nicht zum absolut geschützten Kernbereich privater Lebensgestaltung.

Eine auf die Überwachung in solchen Fällen gerichtete gesetzliche Ermächtigung müsse aber unter Beachtung des Grundsatzes der Normenklarheit nähere Sicherungen der Unantastbarkeit der Menschenwürde enthalten. Das Risiko ihrer Verletzung sei auszuschließen.

C. Datenschutz und Datensicherheit im RBB

I. Regelungen

1. Geschäftsordnung

Darauf, dass die Themen „Datenschutz und „Datensicherheit“ einen hohen Stellenwert beim RBB haben, weist schon die Geschäftsordnung (GO) hin. Sie widmet diesen Themen eine eigene, sehr umfangreiche Regelung.

§ 31 GO lautet:

„Datenschutz und Datensicherung

(1) *Alle fest angestellten und freien Mitarbeiter/innen des RBB sowie Aushilfen, Praktikantinnen/Praktikanten und sonstige Personen, die im Rahmen ihrer Tätigkeit im RBB Zugang zu personenbezogenen Daten haben, sind zu Beginn ihrer Tätigkeit schriftlich auf das Datengeheimnis nach § 8 BInDSG zu verpflichten. Zuständig hierfür ist die HA Personal.*

(2) *Für die Zulässigkeit und Ordnungsgemäßheit der Verarbeitung personenbezogener Daten ist die Leiterin/der Leiter der jeweiligen Organisationseinheit verantwortlich.*

(3) Soweit personenbezogene Daten in nicht automatisierten Verfahren oder in Akten verarbeitet werden, ist die Leiterin/der Leiter der jeweiligen Organisationseinheit verantwortlich für die zur Gewährleistung des Datenschutzes nach § 5 BlnDSG erforderlichen technischen und organisatorischen Maßnahmen. Sie/er hat insbesondere die Maßnahmen zu treffen, die geeignet und erforderlich sind, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung und dem Transport der entsprechenden Unterlagen zu verhindern. Unterlagen mit personenbezogenen Daten, die aus dienstlichen Gründen nicht mehr benötigt werden, sind qualifiziert zu vernichten.

(4) Soweit personenbezogene Daten in automatisierten Verfahren verarbeitet werden, sind für die technischen und organisatorischen Maßnahmen nach § 5 BlnDSG neben der Leiterin/dem Leiter der jeweiligen Organisationseinheit der/die Betreiber/in sowie die für den technischen Zugang zum Verfahren zuständigen Organisationseinheit verantwortlich.

(5) Vor der Entscheidung über den Einsatz oder die Änderung der automatisierten Verarbeitung der Daten muss die für das Verfahren zuständige Organisationseinheit auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzeptes die gemäß § 5 BlnDSG zu treffenden technischen und organisatorischen Maßnahmen ermitteln. Verfahren, die mit besonderen Risiken für Rechte und Freiheiten der Betroffenen verbunden sind, dürfen erst eingeführt werden, nachdem im Rahmen einer Vorabkontrolle gemäß § 19 a Abs. 1 Ziff. 1 BlnDSG die/der Datenschutzbeauftragte die Wirksamkeit der technischen und organisatorischen Maßnahmen geprüft hat.

(6) Die Beschreibung und Verzeichnisse der beim RBB eingesetzten automatisierten Verfahren und der damit verarbeiteten Dateien i.S.v. § 19 BlnDSG führt die/der Datenschutzbeauftragte.

(7) Für Auskünfte und Benachrichtigungen gemäß § 16 BlnDSG über die beim RBB gespeicherten personenbezogenen Daten, den Zweck und die Rechtsgrundlage der Speicherung sowie die Herkunft der Daten und die Empfänger von Übermittlungen ist die Leiterin/ der Leiter der jeweiligen Organisationseinheit zuständig. In Zweifelsfällen ist die/der Datenschutzbeauftragte hinzuzuziehen.

(8) Einzelheiten zur Sicherung von Datenschutz und Datensicherheit im RBB ergeben sich aus einer Dienstanweisung.

(9) Für die Überwachung der Einhaltung der für den RBB maßgeblichen Datenschutzvorschriften ist die/der Datenschutzbeauftragte des RBB zuständig. Sie/er ist dabei von allen Bereichen des RBB zu unterstützen.

(10) Für die Erstellung und Fortschreibung der Datensicherheitskonzepte und die Kontrolle der Umsetzung der darin vorgesehenen Maßnahmen ist ein/e IT-Sicherheitsbeauftragte/r verantwortlich. Sie/er ist dabei von allen Bereichen des RBB zu unterstützen.

2. Sonstige Regelungen

Weitere RBB-interne allgemeine Regelungen, die die Themen Datenschutz und Datensicherheit betreffen (z. B. Datenschutz-, PC-, TK- Richtlinie u. ä.), sind noch nicht erarbeitet worden. Dies hängt vor allem damit zusammen, dass die Personalentscheidungen in der zuständigen Produktions- und Betriebsdirektion erst Anfang 2004 gefallen sind. Da die Verantwortlichen für die Bereiche inzwischen feststehen, gehe ich davon aus, dass jetzt zügig die erforderlichen Regelungen unter meiner Mitwirkung erarbeitet werden können.

Bis dahin sind sinngemäß die ehemaligen einschlägigen Regelungen von ORB und SFB weiterhin maßgeblich.

II. Aktuelle IT-Projekte

1. Lotus notes

Zum leichteren Austausch von E-Mails, Terminen und anderen Informationen beabsichtigt der RBB eine sog. Groupware einzusetzen.

Bei dem bevorstehenden Customizing (RBB-spezifische Konfiguration) wird insbesondere bei der Kalenderfunktion, die u. a. für Gruppen eine gemeinsame Nutzung vorsieht, darauf zu achten sein, dass lediglich Felder eröffnet und Angaben möglich werden, die tatsächlich für den jeweiligen Zweck erforderlich sind. Außerdem müssen für die Nutzung des Kalenders Kriterien vereinbart werden, die dem Arbeitnehmerdatenschutz Rechnung tragen.

2. Spamfilter

Während der Einsatz von Antivirusprogrammen bereits seit Jahren zum Standard gehört, erfordert die täglich größer werdenden Flut von unerwünschten Werbe-Mails (sog. Spam) den Einsatz eines zusätzlichen Instruments: eines sog. Spamfilters.

In technischer Hinsicht erfolgt das Erkennen von Spam überwiegend durch den Einsatz lernfähiger Filter. Diese bauen in der Regel hierarchisch aufeinander auf, indem sie – angefangen bei den Kontrolldaten einer E-Mail (dem sog. Header) bis hin zur Überprüfung ihres

Inhalts (des sog. Body) – anhand verschiedener Kriterien versuchen, die Nachricht als legitim oder unerwünscht zu qualifizieren. Darüber hinaus werden Spam-Datenbanken (sog. „Blacklists“) erstellt, die dazu dienen, unerwünschte E-Mails bereits anhand der IP-Adresse des Absenders zu erkennen und auf diese Weise zu blockieren.

Der geplante Einsatz eines Spam-Filters beim RBB ist erforderlich und auch verhältnismäßig. Andererseits muss dabei das Telekommunikationsgeheimnis beachtet werden. Der Verstoß gegen die rechtlichen Rahmenbedingungen kann unter Umständen sogar strafrechtliche Relevanz haben. Zusammen mit den Verantwortlichen erarbeite ich derzeit Lösungen, die den rechtlichen Anforderungen Rechnung tragen und die Interessen des Betriebes mit denen der Mitarbeiterinnen und Mitarbeiter in Einklang bringen.

III. Sonstiges

1. SAP

Beim RBB wird die Software SAP eingesetzt.

Nachdem die Dienstvereinbarungen von ORB und SFB über den Einsatz der einzelnen SAP-Module mit der Fusion der Sender außer Kraft getreten sind, ist es notwendig, neue Vereinbarungen zu treffen.

Zum Beginn des Jahres 2004 sind für die Personaldatenverarbeitung die bis dahin in zwei verschiedenen Mandanten (getrennt nach ehemals ORB und SFB) genutzten SAP-Module HR (Human Ressource) in einem gemeinsamen Mandanten zusammen geführt worden.

Über die Anwendung des SAP-Moduls HR ist inzwischen unter meiner Mitwirkung eine Dienstvereinbarung abgeschlossen worden, in der – wie in den bisherigen Dienstvereinbarungen für ORB und SFB - die zulässigen Auswertungen und Protokollierungen im Einzelnen festgelegt sind.

Entsprechende Regelungen sind für den Einsatz der weiteren SAP-Module (KMH, FI/FI AA, CO/PS/EC und MM) erforderlich.

2. Kuvertierung der Gehalts- und Reisekostenabrechnung

Mitte 2003 wurde das Verfahren beim Versand von Gehalts- und Reisekostenabrechnungen vom Versand in sog. Taschen auf eine Beförderung in verschlossenen Briefumschlägen umgestellt. Auslöser für die Veränderung war die Notwendigkeit beim Informationsverarbeitungszentrum (IVZ), einen neuen Drucker für die Abrechnungen anzuschaffen. Bei dessen Auswahl spielten in erster Linie Wirtschaftlichkeitsaspekte eine Rolle, aber auch der Datenschutz wurde bedacht.

Die Wahl fiel auf einen Hochleistungs-Laserdrucker, der die Abrechnungen auf Blankopapier ausdruckt. Diese werden anschließend vor Ort im Rechenzentrum kuvertiert und danach an das Gehaltsbüro zur Verteilung gegeben.

Diese Umstellung löste bei einigen Kolleginnen und Kollegen und beim Personalrat Sicherheitsbedenken aus.

Ich habe mich im IVZ vor Ort von der Einhaltung von Datenschutz und Datensicherheit bei jedem einzelnen Arbeitsschritt überzeugen können. Außerdem habe ich die Umstellung zum Anlass genommen, in einem Schreiben an alle Verteiler von Gehalts- und Reisekostenabrechnungen daran zu erinnern, dass insbesondere auch auf eine sichere Verwahrung der Abrechnungen bis zur persönlichen Übergabe an den/die Empfänger/in geachtet werden muss.

3. Überprüfungen durch die Birtler-Behörde

Der Rundfunkrat hat in seiner Sitzung am 8. September 2003 die Empfehlung ausgesprochen, eine Überprüfung aller programmprägenden oder leitenden fest angestellten sowie der programmprägenden freien Mitarbeiter des RBB auf eine etwaige Zusammenarbeit mit dem Ministerium für Staatssicherheit der DDR zu veranlassen.

Dies betrifft sowohl die hauptamtliche/offizielle als auch die inoffizielle Mitarbeit (IM).

Die Geschäftsleitung hat entschieden, der Empfehlung des Rundfunkrates zu folgen. Derzeit wird unter meiner Mitwirkung ein Verfahren für die Durchführung der Überprüfung erarbeitet.

4. Bebildertes Telefonbuch im Intranet

Im Zuge der Erstellung der neuen RBB-Hausausweise wurde im Integrationsbüro die Idee entwickelt, die in diesem Zusammenhang digital erstellten Fotos auch für ein bebildertes Telefonbuch im Intranet zu nutzen. Die Geschäftsleitung hat diese Idee übernommen.

Ich habe darauf hingewiesen, dass die Veröffentlichung der Fotos im Intranet jeweils das Einverständnis der Mitarbeiterinnen und Mitarbeiter voraussetzt. Mein Hinweis ist beachtet worden. Von denjenigen Personen, die ihr Einverständnis nicht erteilt haben, ist kein Foto im Netz.

D. Datenschutz bei der Rundfunkteilnehmer-Datenverarbeitung

I. Allgemeines

Gemäß § 8 Abs. 2 Satz 1 Rundfunkgebührenstaatsvertrag (RGebStV) zieht die GEZ die Rundfunkgebühren für die Landesrundfunkanstalten ein und verarbeitet für diese als Auftragnehmer die beim Gebühreneinzug anfallenden personenbezogenen Daten. Die Datenschutzkontrolle richtet sich nach dem für die jeweilige Anstalt geltenden Recht. Gemäß § 8 Abs. 2 Satz 2 RGebStV bestellt die GEZ einen betrieblichen Datenschutzbeauftragten.

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.

Der größte Anteil der Anfragen betraf auch im Berichtszeitraum wieder die Herkunft der Daten bzw. die Berechtigung zur Datenerhebung. Daneben gab es auch wieder eine Reihe von Anfragen der Finanzämter, die unter Bezug auf § 93 a AO Auskunft über die bei der GEZ gespeicherten Bankverbindungen der Rundfunkteilnehmer zum Zwecke der Vorstreckung bei Steuerschulden haben wollten.

Mit Hinweis auf den Grundsatz der Zweckbindung, der für die Verarbeitung der Rundfunkteilnehmerdaten gemäß § 3 Abs. 3 RGebStV gilt, wurden Auskünfte – wie bisher – regelmäßig versagt.

II. Projekt „2005“ bei der GEZ

Derzeit findet bei der GEZ eine grundlegende Umgestaltung der DV-Architektur statt (Projekt "DV 2005"). Abgelöst werden soll dabei ein vor 25 Jahren entstandenes DV-System, an dem in der Vergangenheit immer wieder Veränderungen, Erweiterungen und Umstrukturierungen vorgenommen worden waren, das aber den gegenwärtigen Anforderungen nur noch schwer gerecht wird. Durch die softwaremäßige Neugestaltung des DV-Systems der GEZ sollen alle bisher ausgeführten Arbeitsabläufe (Teilnehmerbetreuung, Gewinnung neuer Teilnehmer, Betreiben von rückständigen Forderungen, Abwicklung des Zahlungsverkehrs, Gebührenplanung usw.) in einem integrierten einheitlichen System ausgeführt werden. Das Projekt, das von den Rundfunkdatenschutzbeauftragten intensiv begleitet wird, beinhaltet nicht die Lösung neuer Aufgabenstellungen. Es werden lediglich für die vorhandenen Funktionen neue technische Möglichkeiten erarbeitet.

III. Erwerb von Anschriften bei privaten Adresshändlern durch die GEZ

Mit werblich-informierenden Schreiben wendet sich die GEZ regelmäßig an Personengruppen, die noch nicht im Teilnehmerbestand registriert sind. Darin erinnert sie an die Pflicht zur Zahlung von Rundfunkgebühren im Falle des Bereithaltens von Rundfunkgeräten zum Empfang. Für den Fall, dass von den Adressaten Geräte zum Empfang bereit gehalten werden, werden diese aufgefordert, ihre Geräte anzumelden.

Neben den Einwohnermeldedaten, die die GEZ im Fall von Umzügen von den Meldeämtern auf der Grundlage von entsprechenden Meldedaten-Übermittlungsverordnungen erhält, verwendet sie auch Adressen, die sie von verschiedenen kommerziellen Anbietern anmietet bzw. ankauft.

Nach einem Abgleich der Adressen gegen den Rundfunkteilnehmer-Datenbestand, die Robinson- und die interne Sperrdatei werden nur die in diesen Dateien nicht registrierten Ad-

ressaten angeschrieben. Alle übrigen Daten werden sofort gelöscht. Nach Abschluss der Mailing-Aktion und Bearbeitung des Rücklaufs werden sämtliche Daten gelöscht.

Diese Mailing-Maßnahmen sind äußerst wirtschaftlich. Mit einer beachtlichen Erfolgsquote daraufhin neu angemeldeter Rundfunkempfangsgeräte wird das Aufkommen an Rundfunkgebühren erheblich gesteigert. Dabei weisen die Mailings, bei denen Adressen privater Adresshändler verwendet werden, ungefähr den selben Nutzen wie die Mailings auf der Basis der Meldedaten auf.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hält die Beschaffung von Adressen bei privaten Adresshändlern durch die GEZ für den RBB für unzulässig, weil es an einer entsprechenden Rechtsgrundlage fehle (s. Jahresbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2003, 149 f) . Diese Rechtsauffassung halte ich für nicht zutreffend. Ich sehe in § 6 Abs. 1 Satz 2 i.V.m. § 9 Berliner Datenschutzgesetz die einschlägige Rechtsgrundlage.

IV. Rückfragen und Erhebung zusätzlicher Daten im Falle von Abmeldungen

Im Jahr 2003 ging die GEZ im Falle von Abmeldungen wegen Verschenkens/Verkauf von Rundfunkempfangsgeräten dazu über, die Teilnehmer aufzufordern, Namen und Anschrift derjenigen Person mitzuteilen, an die das Gerät abgegeben worden war. Zwar enthielt das Schreiben der GEZ den Hinweis auf die Freiwilligkeit der Angabe. Gleichwohl wurde in dem selben Schreiben aber darauf hingewiesen, dass bis zur Beantwortung der Fragen die gewünschte Abmeldung zunächst noch nicht durchgeführt werde, und damit suggeriert, dass der Rundfunkteilnehmer zu einer diesbezüglichen Auskunft verpflichtet sei.

Derartige Rückfragen sind datenschutzrechtlich nicht zulässig. Eine freiwillige Preisgabe von Daten Dritter ist im datenschutzrechtlichen Sinne nicht möglich.

Nachdem mir diese Praxis bekannt geworden war, habe ich das Thema mit den Datenschutzbeauftragten der anderen Landesrundfunkanstalten erörtert. Der AK DSB, der sich meiner datenschutzrechtlichen Bewertung anschloss, hat daraufhin eine Unterarbeitsgruppe damit beauftragt, sämtliche Formschriften, die bei der GEZ im Falle von Abmeldungen verwendet werden, auf ihre datenschutzrechtliche Zulässigkeit zu überprüfen. Inzwischen

hat die Unterarbeitsgruppe, der ich angehörte, ihre Arbeit erledigt und in einigen Fällen Änderungen empfohlen. Diese Empfehlungen werden jetzt von der GEZ umgesetzt.

E. Datenschutz im journalistisch-redaktionellen Bereich

I. Redaktionssystem „iNews“

Im Februar 2004 wurde an den Standorten Berlin und Potsdam als Ersatz für die veralteten Nachrichtenverteilerprogramme BASYS und D´ACCORD das moderne Redaktionssystem „iNews“ eingeführt.

„iNews“ unterstützt Redaktion und Technik bei Recherche, Sendeplanung und Sendeablauf. Die redaktionellen Arbeitsabläufe werden im Redaktionssystem transparent für alle Mitarbeiterinnen und Mitarbeiter dargestellt. Änderungen und Korrekturen in der Planung, in den Beiträgen oder am Sendeplan sind sofort an allen Arbeitsplätzen nachzuvollziehen. In der Regie wird die Sendung direkt vom Bildschirm gefahren. Durch das Redaktionssystem wird die Regiebesetzung ständig detailliert über Änderungen im Sendeablauf informiert. Jede Berufsgruppe hat eine speziell auf ihre Bedürfnisse hin angepasste Benutzeroberfläche, in der die senderelevanten Informationen übersichtlich dargestellt werden. Durch diese Vernetzung der Regie kann der Redaktionsschluss bis in die Sendung hinein verlagert werden.

Angeschlossene Arbeitsbereiche wie Archive, Fernseh-Produktion etc... erhalten durch „iNews“ eine inhaltliche Erschließung der Sendungen und damit eine echte Arbeitserleichterung.

Ich wurde in der Erprobungsphase mit einbezogen. Eine Vorabkontrolle wurde durch meinen Stellvertreter, Herrn Mohr, durchgeführt. Herr Mohr hat eine Reihe von Anforderungen für das Nutzerkonzept aufgelistet, deren Einhaltung uns zugesagt worden ist.

II. „Schwarze Liste“ bei Antenne Brandenburg

Anfang Januar 2004 war in verschiedenen Berliner und Brandenburgischen Tageszeitungen etwas über die Existenz einer angeblichen „schwarzen Liste“ bei Antenne Brandenburg mit Namen und Adressen von Personen, die bei Gewinnspielen nicht mehr berücksichtigt werden sollten, zu lesen.

Nachdem der Landesbeauftragte für Datenschutz des Landes Brandenburg, Herr Dr. Dix, der Intendantin am 19. Dezember 2003 telefonisch mitgeteilt hatte, dass er das angebliche Führen einer „schwarzen Liste“ bei Antenne Brandenburg vor Ort überprüfen wolle, wies ich diesen noch am selben Tag per Telefax vom 19. Dezember 2003 darauf hin, dass dieser Vorgang ausschließlich in meine Zuständigkeit falle.

Die Aufklärung des Sachverhalts hat ergeben, dass es eine Liste mit Gewinnern der im Programm von „Antenne Brandenburg“ durchgeführten Gewinnspielen gegeben hat.

In einem ausführlichen Gespräch mit dem Chefredakteur von Antenne Brandenburg habe ich diesem deutlich machen können, dass grundsätzlich nur eine zeitweilige Speicherung der Adressen der Gewinner für die Abwicklung des Gewinnspiels (u.a. für die Zusendung des Gewinns) und für Revisionszwecke infrage kommt. Eine Verwendung der Liste für andere Zwecke ist hingegen unzulässig.

Durch technische Maßnahmen (u.a. Berechtigungskonzept) und eine entsprechende Dienstanweisung, flankiert durch eine ergänzende datenschutzrechtliche Unterweisung der Mitarbeiterinnen und Mitarbeiter der Redaktion durch mich, ist jetzt sichergestellt, dass die Daten ausschließlich für die genannten Zwecke und ausschließlich von den damit befassten Personen verwendet werden. Nach Abschluss des Vorgangs werden die Daten jeweils gelöscht.

Die Sache hatte ein Nachspiel:

Mit Schreiben vom 18. Februar 2004 machte Herr Prof. Garstka gegenüber der Intendantin deutlich, dass er in dieser Angelegenheit auf seiner Kontrollbefugnis bestehe. Die Intendantin hat ihm mit Schreiben vom 27. Februar 2004 geantwortet und ihm mitgeteilt, dass auch sie hier die Zuständigkeit der Datenschutzbeauftragten des RBB sehe, da Gewinnspiele ein wesentlicher Bestandteil der redaktionellen Arbeit darstellten. Auf ihre Bitte habe ich

allerdings Herrn Prof. Garstka mit Schreiben vom 2. März 2004 über die von mir ergriffenen Maßnahmen informiert.

Ich hoffe, dass die Landesdatenschutzbeauftragten von Berlin und Brandenburg die Angelegenheit nunmehr auf sich beruhen lassen.

III. Zuschauerredaktion

Zeitgleich mit dem Start des neuen 3. Fernsehprogramms Ende Februar 2004 ist eine Zuschauerredaktion mit Sitz in Babelsberg gegründet worden, deren Aufgabe es in erster Linie ist, Anfragen von Zuschauern des RBB zu beantworten. Mittelfristig sollen jedoch auch neue Formen der Zuschauerbindung entwickelt werden.

Auf Einladung der Leiterin habe ich den Mitarbeiterinnen und Mitarbeitern der Redaktion in einem Gespräch die Grundzüge des Datenschutzrechts erläutert und mit ihnen zusammen Regeln für den Umgang mit den personenbezogenen Daten der Anruferinnen und Anrufer festgelegt. Danach sind grundsätzlich sämtliche Daten nach Erledigung der Anrufe aus dem von der Redaktion genutzten EDV-System zu löschen. Die Nutzung dieser Daten auch für andere Zwecke (z.B. für einen Informationsservice über das RBB- Fernsehprogramm) kommt nur dann in Betracht, wenn die Anrufer dazu eine rechtswirksame Einwilligung im Sinne des Berliner Datenschutzgesetzes erteilt haben.

IV. Versteckte Kamera

Vereinzelt im Berichtszeitraum wahrzunehmenden Tendenzen, die sog. versteckte Kamera als ein normales Mittel der Recherche einzusetzen, bin ich – auch wenn es sich in erster Linie um ein Problem des allgemeinen Persönlichkeitsrechts handelt und das Datenschutzrecht eher am Rande betroffen ist - auch in meiner Eigenschaft als Datenschutzbeauftragte entschieden entgegen getreten.

F. Datenschutz im Informationsverarbeitungszentrum (IVZ)

I. Allgemeines

MDR, RBB, NDR, SR und DLR (die drei letztgenannten als Teilkooperationspartner) betreiben als gemeinschaftliche Einrichtung das Informations-Verarbeitungs-Zentrum (IVZ) im Rahmen einer öffentlich-rechtlichen nicht-rechtsfähigen Verwaltungsgemeinschaft mit Sitz beim RBB.

Gegenstand ist u.a. die Erfassung, Verarbeitung und Nutzung von Daten, einschließlich der Verarbeitung und Nutzung von Daten zu eigenen journalistisch-redaktionellen Zwecken der Rundfunkanstalten, der Einrichtung von Datenbanken, der Programmerstellung und Software-Entwicklung sowie der Durchführung von Arbeiten im Bereich betriebswirtschaftlicher und archivarischer EDV-Anwendungen für die Rundfunkanstalten.

Für die Datenschutzkontrolle beim IVZ sind alle Rundfunkdatenschutzbeauftragten der beteiligten Rundfunkanstalten zuständig. Wie üblich bei ARD-Gemeinschaftseinrichtungen wurde die Federführung für die Datenschutzkontrolle vor Ort mir als der Datenschutzbeauftragten der beteiligten Sitzanstalt übertragen.

In Grundsatzangelegenheiten beziehe ich die Kolleginnen und Kollegen der anderen Rundfunkanstalten ein. Außerdem finden regelmäßig (durchschnittlich ca. einmal pro Jahr) Zusammenkünfte aller beteiligten Rundfunkdatenschutzbeauftragten beim IVZ statt.

II. Einzelne Projekte

1. IVZ-Request

Es ist beabsichtigt, im IVZ ein Change Management einzuführen. Dafür soll die Software „IVZRequest“ genutzt werden. „IVZRequest“ dient der einheitlichen Erfassung, Steuerung und Dokumentation von Aufträgen, die an das IVZ von den beteiligten Rundfunkanstalten erteilt werden. Die Software soll eingesetzt werden, um bestehende Abläufe (z.B. Excel-Listen, Zettel, E-Mail) abzulösen.

Zusammen mit dem IT-Sicherheitsbeauftragten habe ich eine Vorabkontrolle des Systems durchgeführt. Durch technische und organisatorische Maßnahmen ist sichergestellt, dass personenbezogene Daten nur insoweit verarbeitet werden, wie sie für die unmittelbare Aufgabenerfüllung erforderlich sind, und dass sie nicht zur Leistungs- und Verhaltenskontrolle herangezogen werden. Die Daten der Userprofile werden im Jahr der Abmeldung gelöscht. Die Meldungsdaten werden zu Revisionszwecken maximal 10 Jahre vorgehalten.

2. Remote-Tool „Netviewer“

Im IVZ soll zur Verbesserung der Nutzerbetreuung und zur Kosteneinsparung das Remote-Tool „Netviewer“ eingesetzt werden.

Mit „Netviewer“ können Mitarbeiter des IVZ in die Lage versetzt werden, den Inhalt des Bildschirms einer Nutzerin/eines Nutzers einer Rundfunkanstalt auf dem eigenen Rechner angezeigt zu bekommen.

Im Allgemeinen beinhalten Remote-Wartungstools die Gefahr, dass dritten Personen unbeabsichtigt Informationen offenbart werden. Der „Netviewer“ benutzt jedoch einen Ablauf zwischen der Rat suchenden Person und dem IVZ, bei dem die betroffene Person bei jedem Arbeitsschritt jeweils festlegen kann, was die andere Person jeweils sehen und tun darf.

Der Vorgang wird stets von der ratsuchenden Person initiiert. Dazu muss diese sich telefonisch im IVZ melden, den „Netviewer-Client“ starten und erhält per Telefon eine Beraternummer, die in der Startmaske des „Netviewers“ einzugeben ist. Danach kann die ratsuchende Person den Schirm der IVZ-Mitarbeiterin/des IVZ-Mitarbeiters sehen, aber (noch) nicht umgekehrt. Damit der Bildschirminhalt der ratsuchenden Person auf dem Bildschirm im IVZ gesehen werden kann, muss sie dies durch einen Mausklick an ihrem eigenen PC ausdrücklich zulassen. Danach ist zunächst nur die Ansicht freigegeben, aber noch kein externer Eingriff möglich. Will die ratsuchende Person weitergehende Rechte (Mausbewegung, Programme starten ...) freigeben, um weitere Hilfe zu bekommen, muss sie jeweils ausdrücklich das betreffende Zugriffsrecht freigeben.

Nach Durchführung einer Vorabkontrolle zusammen mit dem IT-Sicherheitsbeauftragten, habe ich den Einsatz dieses Tools befürwortet. Bedingung ist allerdings, dass Berater und Nutzer zuvor über die Möglichkeiten und Risiken dieses Instruments umfassend informiert werden.

G. Datenschutz im ARD-Hauptstadtstudio (HSB)

Für die Kontrolle der Einhaltung des Datenschutzes im ARD-Hauptstadtstudio sind alle Datenschutzbeauftragten der ARD-Anstalten gemeinsam zuständig. Die Zuständigkeit für das „Tagesgeschäft“ liegt bei der Datenschutzbeauftragten des RBB.

Das Hauptstadtstudio übernimmt regelmäßig die Regelungen des RBB (ehemals SFB) zu Datenschutz und Datensicherheit. An deren Erarbeitung werden die IT-Verantwortlichen des HSB daher beteiligt.

Im Sommer 2003 ist das Hauptstadtstudio auf das Betriebssystem „WIN-XP“ migriert. Der IT-Sicherheitsbeauftragte und ich wurden in den Prozess mit eingebunden.

H. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Die Datenschutzbeauftragten von ARD, ZDF und DLR arbeiten im Arbeitskreis der Datenschutzbeauftragten (AK DSB) zusammen. Ein wesentliches Ziel des Arbeitskreises ist es, den Datenschutz in den einzelnen Häusern nach möglichst einheitlichen Kriterien sicherzustellen. Darüber hinaus begleitet der Arbeitskreis auch die Gesetzgebung, soweit Datenschutz und Datensicherheit im Rundfunk betroffen sind.

Im Jahr 2003 fanden zwei reguläre Sitzungen des AK DSB, und zwar am 8./9. Mai bei der GEZ in Köln und am 27./28. November beim RBB in Potsdam statt.

Für die Jahre 2004 und 2005 ist der Datenschutzbeauftragte des SWR, Herr Prof. Herb, zum Vorsitzenden des Arbeitskreises und ich zu seiner Stellvertreterin gewählt worden.

Durch den Datenschutzbeauftragten des Norddeutschen Rundfunks wird der AK DSB in der Arbeitsgruppe nach Art. 29 EU-Datenschutzrichtlinie, der alle Datenschutzkontrollstellen der Mitglieder der Europäischen Union angehören, vertreten. Am 11. Februar 2004 wurde der neue Bundesbeauftragte für den Datenschutz, Herr Peter Schaar, für die Dauer von zwei Jahren zum neuen Vorsitzenden der „29er-Gruppe“ gewählt.

2. Ad hoc-Arbeitsgruppe IT- Sicherheit im ARD-CN

Die ARD betreibt mit dem ARD-Daten-Corporate Network einen Datenverbund zwischen den Landesrundfunkanstalten. Um die Kriterien der IT-Sicherheit, Verfügbarkeit, Vertraulichkeit und Integrität zu gewährleisten, sind ARD-übergreifende Mindeststandards für die IT- Sicherheit zu erarbeiten. Zwar ist der CN-Betrieb selbst weitestgehend sicher, jedoch können Anwendungen und Dienste durch die unterschiedlichen Sicherheitsstandards der einzelnen beteiligten Rundfunkanstalten kritisch sein. Der Sicherheitsstandard im CN insgesamt ist nur so hoch, wie derjenige der Anstalt mit dem geringsten Sicherheitsniveau. Daraus resultiert, dass die Sicherheit auch für die Inhalte auf dem Daten-CN nicht von den anstaltsinternen Sicherheitspolicies getrennt werden kann.

Im Herbst 2002 wurde auf ARD-Ebene eine interdisziplinäre Arbeitsgruppe damit beauftragt, eine Erhebung zur IT-Sicherheit in den einzelnen Häusern durchzuführen und Sicherheitsrichtlinien für das ARD-Daten-CN zu erarbeiten. Ich gehöre der Arbeitsgruppe als Vertreterin des AK DSB an.

III. Teilnahme an Veranstaltungen

Am 30. Juni 2003 habe ich an einer Fachkonferenz der Friedrich-Ebert-Stiftung in Berlin zum Thema „Wie geht es weiter im Datenschutz? Die nächsten rechtspolitischen Schritte“ teilgenommen.

Am 9./10. September 2003 hat die zentrale Fortbildungseinrichtung von ARD und ZDF „ZFP“ in Kooperation mit dem AK DSB ein Seminar zum Datenschutz im Rundfunk in Bonn veranstaltet. Neben anderen Kollegen aus dem AK DSB nahm auch ich als Referentin an der Veranstaltung teil. Mit meinem Referat habe ich die Themen „Datenschutz in der Redaktion/datenschutzrechtliches Medienprivileg“ und „Datenschutz bei Online-Angeboten und Gewinnspielen“ abgedeckt.

Berlin, 27. April 2004

Anke Naujock