Zwanzigster Bericht

über die

Tätigkeit des Beauftragten des Saarländischen Rundfunks für Datenschutz

gemäß § 11 Abs. 8 Satz 5 Saarländisches Mediengesetz (SMG)

für die Kalenderjahre 2005 und 2006

Die in diesem Bericht verwendeten personenbezogenen Bezeichnungen gelten für Frauen in der weiblichen und für Männer in der männlichen Sprachform.

Inhaltsverzeichnis:

I. Vorbemerkung

Der Beauftragte für den Datenschutz erstattet dem Intendanten, dem Verwaltungsrat und dem Rundfunkrat jeweils für zwei Kalenderjahre einen Bericht über seine Tätigkeit. Seinen Bericht übermittelt er auch dem Landesbeauftragten für den Datenschutz (vgl. § 11 Abs. 8 Satz 5 SMG). Damit richtete sich der Bericht des Rundfunkdatenschutzbeauftragten – vermittelt über die gesellschaftlich relevanten Gruppen, die im Saarländischen Rundfunk als Interessenwalter der Allgemeinheit tätig sind – bereits seit Jahrzehnten auch an die Allgemeinheit.

Der vorliegende Bericht für den Zeitraum 2005 bis 2006 wird nun erstmalig auch im Internet-Angebot des Saarländischen Rundfunks zugänglich gemacht. Die Publikation des Berichts im Internet trägt einer Reihe von Nachfragen ebenso Rechnung wie dem Umstand, dass eine offene Gesellschaft sich des Internets zunehmend auch als Informationsvermittler bedient.

Wie in der Vergangenheit hat Frau Pia Grossmann den Datenschutzbeauftragten auch in diesem Berichtszeitraum und bei der Abfassung dieses Berichts unterstützt. Sie nimmt ihre Aufgaben im Datenschutzreferat neben ihrer Tätigkeit im Fachbereich Honorare und Lizenzen, also im Nebenamt, wahr. Dabei ist sie mit Aufgaben in der Zuständigkeit des Datenschutzbeauftragten befasst, soweit er sich diese nicht selbst vorbehält.

Das Referat Datenschutz versteht seine Aufgaben nicht vornehmlich kontrollierend, sondern vor allem beratend. Dadurch ist es auch im Berichtszeitraum gelungen, förmliche Beanstandungen auszuschließen. Das ist nicht zuletzt ein Verdienst der regelmäßig kooperationsbereiten Mitarbeiterinnen und Mitarbeiter des SR, die sich bei vielen Vorhaben, die auch nur datenschutzrechtliche Relevanz haben könnten, bereits rechtzeitig melden und bereit sind, dem Rat der „Datenschützer“ zu folgen.

Im öffentlich-rechtlichen Rundfunk ist Datenschutz indessen nicht nur ein Thema des Beauftragten des Saarländischen Rundfunks für Datenschutz. Ebenso wie er unabhängig für den Datenschutz im Unternehmen Saarländischer Rundfunk steht, steht der Saarländische Rundfunk als Medienhaus für eine unabhängige Berichterstattung über datenschutzrelevante Themen.

Die Nutzung biometrischer Daten – etwa zur Gesichtserkennung, die Übermittlung von Fluggastdaten an US-amerikanische Behörden, die Nutzung des Autobahnmautsystems zu Zwecken der Rasterfahndung oder die Videosicherung öffentlicher Orte zu Zwecken der Kriminalitätsbekämpfung sind daher nicht nur Themen, die den Datenschutzbeauftragten sondern auch den Saarländischen Rundfunk als Medium und Faktor der freien Meinungsbildung betreffen und im Berichtszeitraum 2005 bis 2006 beschäftigt haben.

II. Entwicklung des Datenschutzrechts

A. Europäische Union

1. *Einleitung eines Vertragsverletzungsverfahrens*

Im Juli 2005 hat die die Europäische Kommission ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Die Kommission ist der Ansicht, dass die Stellung der Aufsichtsbehörden für den nicht-öffentlichen Bereich in allen 16 Bundesländern gegen Art. 28 der Datenschutzrichtlinie 94/46/EG verstößt. Art. 28 schreibe eine „völlige Unabhängigkeit" der Aufsichtsbehörden vor, insoweit sei die Europäische Datenschutzrichtlinie in Deutschland nicht umgesetzt.

In ihrer Stellungnahme gegenüber der Kommission hat die Bundesregierung die Auffassung vertreten, dass das System der Datenschutzkontrolle im nicht-öffentlichen Bereich durch die Datenschutzrichtlinie nicht habe verändert werden sollen. Eine gerichtliche Auseinandersetzung zwischen der Kommission und der Bundesregierung steht zu erwarten.

2. *Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 zur Vorratsdatenspeicherung von Kommunikationsdaten*

Die Richtlinie zur Vorratsdatenspeicherung von Kommunikationsdaten soll der Harmonisierung der Vorschriften der Mitgliedsstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsdatenspeicherung bestimmter Daten, die von ihnen erzeugt oder bearbeitet werden, dienen. Es soll sichergestellt werden, dass diese Verbindungsdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Nicht betroffen sind Daten, die Aufschluss über den Inhalt der Kommunikation geben. Die Mitgliedsstaaten sorgen dafür, dass die in Artikel 5 der Richtlinie angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.

Die zeitlich befristete Speicherung folgt dem sowohl in der Europäischen Datenschutzrichtlinie als auch in den deutschen Datenschutzgesetzen niedergelegten Grundsatz, personenbezogene Daten zu löschen, sobald sie nicht mehr benötigt werden.

Die Bundesrepublik Deutschland hat sich vorbehalten, die Anwendung dieser Richtlinie – soweit sie die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail betrifft – für einen Zeitraum von 18 Monaten ab dem in Artikel 15 Abs. 1 Satz 1 genannten Zeitpunkt (bis zum 15. März 2009) zurückzustellen. Andere Mitgliedsstaaten haben bereits Rechtsvorschriften über eine verdachtsunabhängige Vorratspeicherung erlassen. Diese nationalen Vorschriften weichen stark voneinander ab.

Die Vorratsdatenspeicherung wie die divergierende Umsetzung der Richtlinie in den einzelnen Mitgliedsstaaten werden nicht nur von Datenschützern, sondern auch von Verfassungs- und von Medienrechtlern kritisch beäugt. Das in der Europäischen Menschenrechtskonvention garantierte Recht auf freie und unbeobachtete Kommunikation könnte verletzt sein. In den Rundfunkanstalten wird zudem der Informanten- und Quellenschutz in Gefahr gesehen.

3. Prümer Vertragsgesetz

Das Prümer Vertragsgesetz ist ein Vertrag zwischen (zurzeit) sieben Mitgliedsstaaten der Europäischen Union. Er regelt die grenzüberschreitende Zusammenarbeit und den Informationsaustausch zwischen den Vertragsparteien zum Zweck der Verhinderung und der besseren Verfolgung von Straftaten. In Deutschland ist der Prümer Vertrag durch Gesetz vom 10. Juli 2006 (Bundesgesetzblatt 2006, Teil I, S. 1458) umgesetzt.

Polizei- und Strafverfolgungsbehörden können direkt auf bestimmte Datenbanken zugreifen, die von den Behörden der anderen Vertragsstaaten geführt werden. Die Zugriffsberechtigung erstreckt sich auf DNA-Analysedaten (eine entsprechende Datenbank wird vom Bundeskriminalamt als „DNA-Datenbank“ unterhalten), Datenbanken mit elektronisch gespeicherten Fingerabdrücken (in Deutschland das „Automatisiertes Fingerabdruckidentifizierungssystem“ AFIS) und elektronische Register mit KFZ-Daten und KFZ-Halterdaten (hier das „Zentrales Fahrzeugregister“ des Kraftfahrt-Bundesamtes).

Die Dateninformationsübermittlungen werden durch sog. Nationale Kontrollstellen durchgeführt. In Deutschland sind dies das BKA oder das Kraftfahrtbundesamt.

B. Bundesrecht

1. Strafprozessordnung (StPO)

Das Bundesverfassungsgericht (BVerfG) hatte mit seinem Urteil vom 3. März 2004 (Az. 1 B VR 2378/98, 1 B 1084/99) zum „Großen Lauschangriff“ festgestellt, dass die einschlägigen Vorschriften der StPO zur akustischen Wohnraumüberwachung den Vorgaben des Art. 13 GG nicht genügten. Es hatte dem Gesetzgeber aufgegeben, einen verfassungsgemäßen Zustand bis spätestens 30. Juni 2005 herzustellen.

Am 1. Juli 2005 ist das „Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung)“ in Kraft getreten. Die akustische Wohnraumüberwachung darf danach nur beim Vorliegen des Verdachts einer besonders schweren Straftat aus dem in § 100c Abs. 2 StPO aufgeführten Katalog angeordnet werden. Wenn sich während der Überwachung Anhaltspunkte für die Erfassung von Äußerungen, die dem privaten Kernbereich zuzuordnen sind, ergeben, ist die Überwachung zu unterbrechen und die Aufzeichnungen darüber sind zu löschen

(§ 100c Abs. 5 StPO). Das Abhören von Berufsgeheimnisträgern, wozu auch die Journalisten gehören, ist gemäß § 100c Abs. 6 StPO unzulässig.

2. *Bundesdatenschutzgesetz (BDSG)*

Durch die aktuelle Änderung des Bundesdatenschutzgesetzes (Bundesgesetzblatt 2006, Teil I, S. 1979ff.) haben sich folgende Veränderungen ergeben:

- Heraufsetzen des sog. Beschäftigten-Schwellenwertes, mit dem die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten begründet wird, auf „mehr als neun" Personen, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Der arbeitsrechtliche Status der Personen ist dabei nicht maßgebend. Auch Praktikanten, Auszubildende, Geschäftsführer etc. zählen zu dem relevanten Personenkreis. Wenn ein Unternehmen aus der Bestellungspflicht aufgrund des Unterschreitens der Personenzahl entlassen wurde, hat die Unternehmensleitung gem. § 4g in anderer Weise für die Einhaltung der datenschutzrechtlichen Bestimmungen zu sorgen. (Dies ist kritisch zu sehen, weil zum einen die vorhandenen Hard- und Softwaremöglichkeiten ignoriert werden und zum anderen der Irrglaube besteht, eine geringe Personenzahl sei mit wenig automatisierter Datenverarbeitung gleichzusetzen.)
- Entfallen der Meldepflicht nach § 4d Abs. 3 BDSG, wenn diese Personenzahl nicht erreicht wird
- Präzisierung des Begriffs „Fachkunde": Das Maß der erforderlichen Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die diese erhebt oder verwendet.
- Erstreckung der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten auch auf Berufsgeheimnisträger wie Ärzte, Rechtsanwälte, Steuerberater und damit verbundene weitere Rechte und Pflichten
- Einräumung eines Beratungsanspruchs des betrieblichen Datenschutzbeauftragten durch die Aufsichtsbehörden

3. *Bundes-Informationsfreiheitsgesetz (IFG)*

Das Gesetz zur Regelung des Zugangs zu Informationen des Bundes (IFG) ist nach langen Beratungen und politischen Kontroversen am 1. Januar 2006 in Kraft getreten. Damit erhält jeder – unabhängig von einer persönlichen Betroffenheit – ein Recht auf freien Zugang zu amtlichen Informationen der öffentlichen Stellen des Bundes. Dieser Anspruch umfasst alle Aufzeichnungen, die amtlichen Zwecken dienen, also sowohl Schriftstücke als auch Daten, die in Computersystemen gespeichert sind. In gewissen Ausnahmefällen, etwa zum Schutz besonderer öffentlicher Belange (z.B. der inneren und äußeren Sicherheit oder der Durchführung von Gerichts- und Ermittlungsverfahren), personenbezogener Daten, des geistigen Eigentums oder von Betriebs- und Geschäftsgeheimnissen dürfen die gewünschten Informationen verweigert werden. Dann muss die Behörde dies begründen, wobei gegen ablehnende Entscheidungen der Rechtsweg möglich ist. Wer sein Recht auf Informationszugang beeinträchtigt sieht, kann sich an den Bundesda-

tenschutzbeauftragten wenden, der gleichzeitig der sog. Bundesbeauftragte für Informationsfreiheit ist. Es erfolgte auch eine Anpassung an das BDSG.

Unter Umständen könnte das IFG bei der verdeckten Recherche für Journalisten nützlich sein. Bei presserechtlichen Auskünften nämlich muss ein besonderes Interesse dargelegt werden.

4. *Telemediengesetz (TMG) / 9. Rundfunkänderungsstaatsvertrag*

Im Bereich der elektronischen Medien gab es die Überlegung, die bestehenden Datenschutzregelungen für Tele- und Mediendienste einheitlich in einem Bundesgesetz zusammenzufassen. Ziel war ein neues „Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG)“ des Bundes, das in Art. 1 ein sog. Telemediengesetz enthalten sollte. Parallel dazu haben die Länder den Mediendienste-Staatsvertrag aufgehoben und entsprechende Regelungen in den Rundfunkstaatsvertrag aufgenommen.

Die Vorschriften für die „Telemedien“ sind derart formuliert dass sie unabhängig vom Verbreitungsweg gelten sowie vereinfacht und entwicklungsoffen ausgestaltet sind. Im TMG werden bestimmte rechtliche Anforderungen im Hinblick auf Telemedien (bisher v .a. im Teledienstgesetz und im Mediendienste-Staatsvertrag geregelt) zusammengefasst, wie z.B. Zugangsfreiheit, Herkunftslandprinzip und Kennzeichnungspflicht. Die an die Inhalte von Telemedien zu richtenden besonderen Anforderungen ergeben sich gemäß § 1 Abs. 4 TMG aus dem Staatsvertrag für Rundfunk und Telemedien, wie der Rundfunksstaatsvertrag jetzt genannt wird. Auch der spezifische Datenschutz für Telemedien mit redaktionellen Inhalten wird in einem eigenen Artikel im neuen Rundfunkstaatsvertrag geregelt.

ARD und ZDF haben das Gesetzgebungsverfahren intensiv begleitet, die Gelegenheit zur Stellungnahme wahrgenommen und auch an der Anhörung teilgenommen. Für die öffentlich-rechtlichen Rundfunkanstalten ist dabei vor allem bedeutsam gewesen, dass dem aus Art. 5 Abs. 1 Satz 2 GG abzuleitenden Medienprivileg sowohl hinsichtlich der materiell-rechtlichen Regelungen als auch bei der Zuordnung der Kontrollkompetenzen (Frage der Aufsicht über die Telemedien) Rechnung getragen wird. Dies wurde letztendlich auch erreicht: Die anstaltsinternen Kontrollzusammenhänge bleiben auch für die Telemedien, insbesondere die Online-Angebote der Rundfunkanstalten, erhalten. Für die Aufsicht über die Telemedien der öffentlich-rechtlichen Rundfunkanstalten sind weiterhin ausschließlich die Anstalten zuständig. Für die Aufsicht über die Einhaltung des Datenschutzes bei den Telemedien sind die Rundfunkdatenschutzbeauftragten zuständig.

Das Telemediengesetz und der 9. Rundfunkänderungsstaatsvertrag sind nicht mehr im Berichtszeitraum in Kraft getreten. Die Europäische Kommission hatte im Rahmen der notwendigen Notifizierung der beiden Gesetzeswerke verschiedene Bedenken geäußert und Bund und Länder zu einer ent-

sprechenden Antwort und Klarstellung aufgefordert. Zwischenzeitlich sind das Gesetz und der Staatsvertrag aber in Kraft getreten.

5. Rechtsprechung zum Datenschutz:

a) *Urteil des Bundesverfassungsgerichts vom 2. März 2006 (Az: 2 BvR 2099/04) über die Bedingungen für die Beschlagnahme von E-Mail- und Handy-Verbindungsdaten*

Hier hat das BVerfG die Bedingungen für die Beschlagnahme von e-Mail und Mobilfunk-Verbindungsdaten erleichtert, soweit diese auf dem Empfangsgerät gespeichert sind. Nach diesem Urteil unterliegen Verbindungsdaten nicht mehr dem Fernmeldegeheimnis, sobald sie beim Empfänger eingegangen sind und der Übertragungsvorgang beendet ist. Gleichwohl müsse die Beschlagnahme entsprechender Daten im Rahmen einer Durchsuchungsaktion „verhältnismäßig" sein und das Recht auf informationelle Selbstbestimmung gewahrt bleiben.

Im Ergebnis reicht nach dieser Rechtsprechung der Verdacht auf eine leichte Straftat aus, um die Verbindungsdaten beim Empfänger zu beschlagnahmen.

Die Beschlagnahme in Redaktionsräumen bzw. Wohnungen von Journalisten bleibt indessen auf Ausnahmefällen beschränkt (§ 97 Abs. 5 StPO).

b) *Beschluss des Bundesarbeitsgerichts (BAG) vom 14. Dezember 2005 (Az: 1 ABR 34/03) zur Videoüberwachung von Mitarbeitern*

Das Bundesarbeitsgericht hatte über die Zulässigkeit der Videoüberwachung in einem Briefverteilzentrum der Deutschen Post AG zu entscheiden. Es stellte fest, dass die Überwachung der Arbeitnehmer am Arbeitsplatz durch eine Videoanlage einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht darstellt Dieser Eingriff könne nur durch überwiegende schutzwürdige Belange des Arbeitgebers gerechtfertigt sein. Jedenfalls das Postgeheimnis, das Eigentum der Postkunden und die wirtschaftlichen Interessen Deutschen Post AG seien nicht geeignet, um die Einschränkung der Arbeitnehmer durch eine bis zu 60 Stunden pro Woche dauernde Videoüberwachung in den nicht öffentlich zugänglichen Arbeitsräumen zu rechtfertigen.

C. Landesrecht

1. *8. Rundfunkänderungsstaatsvertrag*

Der 8. Rundfunkänderungsstaatsvertrag ist zum 1. April 2005 in Kraft getreten. Aus datenschutzrechtlicher Perspektive sind vor allem folgende Änderungen im Rundfunkgebührenstaatsvertrag (RGebStV) bedeutend:

- § 6 Abs. 2 RGebStV: Nachweis der Voraussetzungen der Befreiungstatbestände

  Die Länder haben den RGebStV mit dem Ziel der Vereinfachung des Verfahrens der Befreiung von der Rundfunkgebührenpflicht und der Vereinheitlichung der Befreiungstatbestände geändert. Anträge auf Befreiung von der Rundfunkgebührenpflicht werden seit dem 1. April 2005 nicht mehr von den einzelnen Sozialbehörden bearbeitet. Die Befreiung wird nicht mehr an komplizierte Einkommensberechnungen geknüpft und der Bürger braucht keine entsprechend aufwändigen Nachweise mehr zu führen. Vielmehr kann der Antragsteller seitdem das Vorliegen der Voraussetzungen für eine Gebührenbefreiung durch die Vorlage entsprechender – ohnedies vorhandener – Bescheide, entweder im Original oder in beglaubigter Kopie, nachweisen. Dies entspricht im Übrigen der bei anderen Sozialleistungen gängigen Praxis. Das bis dahin gültige Befreiungsverfahren hatte sich am tatsächlichen Einkommen des beantragenden Teilnehmers orientiert und war entsprechend nachweis- und bearbeitungsintensiv. Die Neuerung war zur Entlastung aller Beteiligten gedacht, führte aber zu vielen Problemen und ist datenschutzrechtlich bedenklich.

- § 8 Abs. 4 RGebStV: Einheitliche Rechtsgrundlage für GEZ-Mailing

  Bereits seit langem führt die GEZ im Auftrag der Rundfunkanstalten zur Hebung der Teilnehmer so genannte Mailings durch. Dabei werden zielgruppenspezifisch Adressen angemietet, um potentielle Rundfunkteilnehmer über die Rundfunkgebührenpflicht zu informieren. Die Adressanmietung war – insbesondere von einzelnen staatlichen Datenschutzbeauftragten – unter Hinweis auf eine vermeintlich fehlende Rechtsgrundlage kritisiert worden. Mit der Vorschrift wird eine für alle Länder einheitliche Rechtsgrundlage für die Datenerhebung der Rundfunkanstalten bzw. der Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ) bei Dritten eingeführt. Bis dahin war die Zulässigkeit der Anmietung von Adressen und der Abgleich mit dem Bestand nach den für die jeweilige Rundfunkanstalt geltenden gesetzlichen Vorschriften (insbesondere den Landesdatenschutzgesetzen) zu beurteilen.

  Obwohl nach dem Willen der Rundfunkgesetzgeber mit § 8 Abs. 4 RGebStV eine einheitliche Norm und eine gesicherte Rechtsgrundlage für die Adressanmietung zu Mailingzwecken beabsichtigt war, ist auch die Neuregelung und die Praxis der Adressanmietung rechtspolitisch

umstritten. Einzelne Landesdatenschutzbeauftragte kritisieren die Regelung als zu weitgehend.

Die staatlichen Landesdatenschutzbeauftragten haben einen Vorschlag zur neuerlichen Änderung des § 8 Abs. 4 RGebStV in die politische Diskussion eingebracht. Die Rundfunkreferenten der Länder haben zwischenzeitlich alle Beteiligten an einen Tisch gebracht, um das Anliegen der staatlichen Landesdatenschutzbeauftragten und einen eventuellen Novellierungsbedarf der gerade erst getroffenen Regelung zu erörtern. Dabei haben die Rundfunkdatenschutzbeauftragten einen bereits im Vorfeld der Beratungen des 8. Rundfunkänderungsstaatsvertrages eingebrachten – aus heutiger Sicht – vermittelnden Regelungsvorschlag nochmals unterbreitet. Danach bliebe es bei der bereits heute zurückhaltenden Praxis, es würde indessen klargestellt, dass die Erforderlichkeit der Datenerhebung streng zweckgebunden zu beurteilen ist.

2. *Saarländisches Datenschutzgesetz (SDSG)*

Das Saarländische Gesetz zum Schutz personenbezogener Daten (Saarländisches Datenschutzgesetz) gilt nach wie vor in der Fassung vom 24. März 1993, zuletzt geändert durch das Gesetz vom 27. Februar 2002.

3. *Saarländisches Mediengesetz (SMG)*

Auch das SMG hat sich im Berichtszeitraum nicht geändert.

4. *Saarländisches Informationsfreiheitsgesetz (SIFG)*

Am 15. September 2006 ist das Saarländische Informationsfreiheitsgesetz (Amtsblatt des Saarlandes vom 14. September 2006, S. 1624 ff.) in Kraft getreten. Mit diesem Gesetz erhält jeder ein Recht auf freien Zugang zu amtlichen Informationen der öffentlichen Stellen des Saarlandes. Dazu gehören beispielsweise die Behörden des Landes, die Gemeinden und Gemeindeverbände. Der gesetzliche Anspruch auf Informationszugang gilt auch für sonstige Organe und Einrichtungen des Landes, der Gemeinden und Gemeindeverbände, soweit diese öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen.

Das SIFG verfolgt den Zweck staatliches Handeln für den Bürger transparenter zu machen. Gleichzeitig erhält die staatliche Verwaltung die Möglichkeit ihr Handeln den Bürgern – im Sinne von mehr Bürgernähe - zu optimieren.

Der Anspruch umfasst alle Aufzeichnungen, die amtlichen Zwecken dienen. Das können Schriftstücke, aber auch Daten, die in Computersystemen gespeichert sind, sein. Der Zugang kann durch Akteneinsicht bei der Behörde, Übersendung von Aktenauszügen in Kopie oder mündliche bzw. schriftliche Auskunft gewährt werden. Hierfür ist ein formloser Antrag ausreichend. Die gewünschten Informationen sind dem Bürger so schnell wie möglich, jedenfalls aber innerhalb von vier Wochen zugänglich zu machen. Dabei können ihm auch Kosten entstehen. Verweigert werden darf der Informati-

onszugang ganz oder teilweise nur in Ausnahmefällen, als da sind der Schutz besonderer öffentlicher Belange (z. B. die innere Sicherheit oder die Durchführung von Gerichts- oder Ermittlungsverfahren), personenbezogener Daten, des geistigen Eigentums oder von Betriebs- und Geschäftsgeheimnissen. Werden die Informationen verwehrt, muss die öffentliche Stelle dies begründen und gegen die ablehnende Entscheidung sind Widerspruch und Klage möglich.

Das SIFG überträgt nach dem Vorbild des (B)IFG die Aufgaben des Landesbeauftragten für Informationsfreiheit dem Landesbeauftragten für Datenschutz. Demzufolge kann sich jeder, der sich in seinem Recht auf Informationszugang nach dem SIFG verletzt sieht, an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden.

Für den Saarländischen Rundfunk ist das Gesetz in zweierlei Hinsicht relevant.

Einerseits hinsichtlich der eigenen Auskunftspflicht gegenüber Bürgern. Hier unterscheidet das Gesetz zutreffend zwischen der Rundfunkanstalt in ihrer Funktion als Medium und Faktor der Meinungsbildung und staatlichen Behörden. Nur in Fällen öffentlich-rechtlichen Verwaltungshandelns ist der Rundfunk – wie eine Behörde – der Auskunft verpflichtet. Denkbar sind insoweit zwei Bereiche in denen ggf. Auskunft zu erteilen ist. Das ist einmal der Rundfunkgebühreneinzug. Zum anderen ist es die Vergabe von Sendezeiten an Dritte. Da der Rundfunkgebühreneinzug durch die individuelle Rundfunkgebührenpflicht einen starken Personenbezug aufweist, ist fraglich, ob dem Bürger hier eine gegenüber dem status quo der Datenschutzgesetzgebung veränderte tatsächliche Auskunftspflicht zusteht, jedenfalls wird die Auskunftspflicht gegenüber dem Jedermann nicht sehr weit gehen dürfen, ohne datenschutzrechtliche Probleme auszulösen. Hinsichtlich der Vergabe von Sendezeiten an Dritte wird die von Verfassungs wegen gebotene Staatsferne des Rundfunks diese Fälle auf wenige Anwendungsfälle reduzieren.

Andererseits geht es um die Auskunftspflicht staatlicher Behörden gegenüber dem Saarländischen Rundfunk. In dieser Hinsicht wird der Rundfunk indessen regelmäßig bereits durch einen presserechtlichen Auskunftsanspruch gegenüber dem Bürger privilegiert, so dass sich der Wert dieses gesondereten Auskunftsanspruchs erst noch erweisen muss. Denkbar sind hier vor allem Anwendungsfälle im Bereich der verdeckten Recherche.

III. Datenschutz beim Saarländischen Rundfunk

1. Treffen mit dem saarländischen Landesbeauftragten für Datenschutz und Informationsfreiheit

Mit Herrn Lorenz, in dessen Zuständigkeitsgebiet neben dem Datenschutz nun auch die Informationsfreiheit fällt, haben sich Frau Grossmann und der Datenschutzbeauftragte des SR im Berichtszeitraum zweimal, und zwar im April 2005 und April 2006 zum Gedankenaustausch und zur Diskussion gemeinsamer interessierender Themen. Dabei hat u. a. die Begleitung des Gesetzgebungsprozesses zum Saarländischen Informationsfreiheitsgesetz breiten Raum eingenommen.

2. Teilnahme an Fortbildungsveranstaltungen

Frau Grossmann nahm an zwei Informations- bzw. Fortbildungsveranstaltungen teil:

- Im Mai 2006 an der Tagung der Alcatel SEL Stiftung für Kommunikationsforschung in Stuttgart zum Thema „Digitale Rechteverwaltung – Eine gelungene Allianz von Recht und Technik“, wo u. a. „Digitale Rechteverwaltung und Datenschutz“, „Rechteverwaltung zwischen Effektivität und Datenschutz“ und „Datenschutzgerechtere Rechteverwaltung“ behandelt wurden
- Im Juni 2006 am 15. Wiesbadener Forum Datenschutz , das sich mit „Informationsfreiheit und Datenschutz“, genauer gesagt dem Verhältnis von Informationsfreiheit und Datenschutz und den Erfahrungen einzelner Bundesländer mit ihren Informationsfreiheitsgesetzen beschäftigte

Diese Veranstaltungen werden besucht, um den Wissens- und Kenntnisstand auf dem notwendigen Niveau zu halten. Gerade im Hinblick auf den Einsatz neuer Techniken ist das Datenschutzrecht ständig im Fluss.

3. Dienstanweisung Datenschutz

Zum 4. April 2005 trat die „Dienstanweisung zum Schutz personenbezogener Daten im SR (sog. Dienstanweisung Datenschutz)“ in Kraft, die im letzten Datenschutzbericht bereits angekündigt worden war.

Sie ist notwendig geworden, weil beinahe jeder Mitarbeiter des SR im Zusammenhang mit seiner dienstlichen Tätigkeit Zugang zu und Umgang mit personenbezogenen Daten anderer hat. Ziel ist dabei, das Recht des Einzelnen zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu entscheiden (Grundrecht auf informationelle Selbstbestimmung).

Den Wortlaut der Dienstanweisung nebst zehn schlagwortartig formulierten Regeln zum sicheren Umgang mit vernetzten Systemen finden Sie als Anlage zu diesem Bericht.

4. Datenschutzrechtliche Anfragen zum Rundfunkgebührendienst

Auch in diesem Berichtszeitraum gab es vereinzelte, im Ergebnis aber nicht begründete Beschwerden zum Rundfunkgebührendienst.

Dabei wandten sich teilweise die Betroffenen direkt an den Datenschutzbeauftragten des SR, teilweise erreichten uns die Eingaben über den Landesbeauftragten für Datenschutz und Informationsfreiheit. In den meisten Fällen genügte die Darlegung der Rechtslage, wie sie sich insbesondere aus dem Rundfunkgebührenstaatsvertrag ergibt, um die Petenten zufrieden zu stellen.

5. Altaktenentsorgung

Ähnlich wie im letzten Berichtszeitraum gab es auch Anfang 2006 – dieses Mal anlässlich der Renovierung des Fernsehgebäudes – eine größere Altaktenentsorgungsaktion, die bereits im Vorfeld vom Referat Datenschutz begleitet wurde. So wurden die externen Hilfskräfte, die an der Entsorgung beteiligt waren, auf den Datenschutz verpflichtet. Die mit der Entsorgung beauftragte Firma ist nach § 32 BDSG eingetragen und vernichtet die Daten nach den einschlägigen DIN-Vorschriften.

Die Aktenvernichtung erfolgte im Berichtszeitraum ohne besondere Vorkommnisse.

6. Dienstvereinbarung über die Einrichtung und den Betrieb von Videosicherungsanlagen beim Saarländischen Rundfunk vom 28. Dezember 2004

Am 28. Dezember 2004 wurde zwischen dem SR und seinem Personalrat eine „Dienstvereinbarung über die Einrichtung und den Betrieb von Videosicherungsanlagen beim Saarländischen Rundfunk“ abgeschlossen. Zwar will und möchte der SR weiterhin ein im Grundsatz offenes Haus bleiben. Dennoch soll das Sicherheitsniveau verbessert werden. SR und Personalrat sehen in der Einrichtung eines Video-Sicherungssystems ein adäquates Mittel hierzu. Eine Verbesserung der persönlichen Sicherheit der Menschen auf dem Halberg, insbesondere in den so genannten Tagesrandzeiten, sowie die Vermeidung von Diebstählen und weiteren Straftaten sind angestrebt.

Gemäß § 9 Abs. 4 der Dienstvereinbarung ist den Belangen des Datenschutzes jederzeit Rechnung zu tragen.

Insbesondere war beabsichtigt, dass die Regelungen dem Grundgedanken des § 34 SDSG, der die Videoüberwachung thematisiert, entsprechen. Die Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen (so die gesetzliche Definition der Videoüberwachung) ist danach nur zulässig, soweit sie zur Wahrnehmung des Hausrechts, zum Zweck des Schutzes von Personen oder Eigentum, des Besitzes oder der Kontrolle von Zugangsberechtigungen oder zur Aufgabenerfüllung der verantwortlichen Stelle erforderlich ist. Zusätzlich dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Der Datenschutzbeauftragte des SR hat zu der Dienstvereinbarung seine Zustimmung erteilt.

Einige Kameras sind mittlerweile in Betrieb. Sie sind durch entsprechende Hinweisschilder gekennzeichnet. Da die Bestückung mit Kameras noch nicht gänzlich abgeschlossen ist, wird dem Thema im nächsten Berichtszeitraum weitere Aufmerksamkeit zu widmen sein.

7. Einzelanfragen aus dem Haus

Wie auch im vorangegangenen Berichtszeitraum wird immer wieder nachgefragt, wie mit beispielsweise aus Gewinnspielen vorhandenen E-Mail-Adressen umgegangen werden kann, insbesondere, ob an diese Newsletter geschickt werden dürfen. Aus programmlicher Sicht wolle man gerne mit den Hörern bzw. mit den Zuschauern kommunizieren. Grundsätzlich müssen allerdings in diesem Fall die potentiellen Empfänger ihr Einverständnis erklären, derartige Newsletter zu erhalten. Auch eine Abbestellmöglichkeit für die Newsletter muss eingeräumt werden. Es wird einerseits die Wichtigkeit solcher Maßnahmen für die Macher des Programms nicht in Abrede gestellt, andererseits muss den Erfordernissen des Datenschutzes Rechnung getragen werden. Konkrete Beschwerden sind aufgrund dieser im Vorfeld mit den Redaktionen geklärten Fragen unserem Referat erfreulicherweise nicht zur Kenntnis gebracht worden.

Das Referat Datenschutz achtet bei Beschäftigung externer Firmen oder Referenten darauf, dass diese auf den Datenschutz verpflichtet werden, sofern sie mit sensiblen Daten umgehen. Hierbei ist wichtig, dass die Bereiche, die solche Firmen verpflichten, sich an unser Referat wenden und die Problematik erkennen. Dasselbe gilt für Diplom- oder Magisterarbeiten, die beim bzw. über den SR geschrieben werden. Die Aufklärungsarbeit hat bewirkt, dass die Akzeptanz des Datenschutzes im Allgemeinen steigt.

Im Zusammenhang mit einer geplanten Fortbildung wurden an Teilnehmer Ende 2006 Fragebögen verteilt, in denen vertrauliche Daten abgefragt wurden. Hier wurde in Zusammenarbeit mit dem Bereich Zentrale Aufgaben, Organisation, Controlling nach einer datenschutzrechtlich verträglichen Lösung gesucht, indem eine anonymisierte bzw. pseudonymisierte Befragung durchgeführt wurde. Dabei hat man die Merkmale, mit deren Hilfe Personenbezug herzustellen gewesen wäre, gesondert gespeichert und nach Erreichung des Zwecks gelöscht, die Fragebögen selbst sofort nach Auswertung vernichtet. Die durchführende Consultingfirma wurde zur Verschwiegenheit verpflichtet.

In Verbindung mit unserem Fuhrpark wurde eine sog. Selbstfahrer-Datenbank begutachtet, die erkennen lässt, welche beim SR beschäftigten Personen über eine Selbstfahrergenehmigung verfügen, um Dienstwagen steuern zu dürfen. Eine derartige Datenbank ist notwendig, weil etwa betriebsärztliche Untersuchungen turnusmäßig wiederholt werden und auch Führerscheindaten hinterlegt werden müssen. Hier wurden die verarbeiteten Daten auf das erforderliche Mindestmaß nach dem Grundsatz der Datensparsamkeit beschränkt.

Des Weiteren wurde im Sachgebiet Licht des SR im Jahr 2006 das Lagerverwaltungsprogramm „easyjob“ eingeführt. Bei der Materialverwaltung und Ausleihe lichttechnischer Geräte wird nun statt handschriftlich geführter Karteien „easyjob“ genutzt. Dem Referat Datenschutz wurde das Programm präsentiert, in dem nur in geringem und unbedingt erforderlichem Rahmen personenbezogene Daten (nämlich die Namen der persönlich bekannten ausleihenden Personen) enthalten sind.

Das Programm WebMerlin befand sich im Berichtszeitraum noch im Projektstatus und wurde datenschutzrechtlich geprüft. WebMerlin ist ein Workflow-Management-System zur Programmplanung, Sendungsvorbereitung und Sendungsabwicklung. Gespeist wird es vor allem von den Hörfunkredaktionen mit planungsrelevanten Daten aus Musik- und Wortbereichen, die Bereiche Fernsehen und Multimedia besitzen nur Lesezugriffe. Je nach Aufgabe gibt es festgelegte Benutzerregeln mit lesenden und/oder schreibenden Rechten auf die im System erhobenen Daten. Der Zugang ist nur mit Benutzerkennung und Passwort möglich. Das Berechtigungskonzept ist administratorgesteuert. In der Verwaltung werden die Ist-Daten als Grundlage für die Honorierung freier Mitarbeiterinnen und Mitarbeiter bzw. zur Weitergabe an die Verwertungsgesellschaften (z.B. GEMA, GVL) in den dafür vorgesehenen angeschlossenen Systemen und zur Erstellung der Sendezeitstatistik verwendet. WebMerlin läuft auf den Servern des IVZ (s. u). und zur Datenübertragung wird ausschließlich das ARD-CN verwendet.

Im Fernsehen wurde FESADneu eingeführt, das ebenfalls auf den IVZ-Rechnern läuft und von einigen anderen Rundfunkanstalten, beispielsweise dem federführenden HR, genutzt wird. Vor allen die Mitarbeiter des Fernseharchivs nutzen die Anwendung in der Erfassungs- und Rechercheperspektive. Erstere dient der Datenerfassung und –änderung, letztere der Anwendung der erfassten Daten für betriebliche Zwecke. Auch hier erfolgt der allgemeine Einstieg zunächst über das SR-Netzwerk mit Hilfe von Benutzerkennung und Passwort, dann über einen sog. gleichfalls passwortgeschützten FESAD-Benutzer. Eine weitere Einstiegsmöglichkeit eröffnet das SR-Intranet über die sog. SAD-Recherche. Auch diese Anwendung wurde bei ihrer Einführung datenschutzrechtlich begleitet.

Im Berichtszeitraum wurde beim SR an einer „Integrationsvereinbarung“ gearbeitet, die zu dessen Ende noch nicht fertig gestellt war. Darunter ist eine Vereinbarung zur Beschäftigung und Integration behinderter Menschen im Saarländischen Rundfunk gemäß § 83 SGB IX zu verstehen. Da die Integration behinderter Menschen eine gesamtgesellschaftliche Aufgabe ist, sieht sich der SR als öffentlich-rechtliches Unternehmen in besonderer Weise verpflichtet, die Beschäftigung behinderter Menschen zu fördern und sie in betriebliche Abläufe zu integrieren. Da es nach den Entwürfen der Integrationsvereinbarung einige Sitzungen geben kann, in denen sensible Gesundheitsdaten der Schwerbehin-

derten eine Rolle spielen, ist das Thema auch datenschutzrechtlich relevant. Auf die Integrationsvereinbarung wird im Detail im nächsten Bericht eingegangen.

8. Datenschutz beim Informationsverarbeitungszentrum (IVZ)

Der SR betreibt gemeinsam mit den Rundfunkanstalten MDR, rbb, NDR, dem Deutschlandradio sowie neuerdings Radio Bremen das IVZ in Berlin. Gegenstand ist die Erfassung, Verarbeitung und Nutzung von Daten, einschließlich der Verarbeitung und Nutzung von Daten zu journalistisch-redaktionellen Zwecken der Rundfunkanstalten, der Einrichtung von Datenbanken, der Programmerstellung und Softwareentwicklung sowie der Durchführung von Arbeiten im Bereich betriebswirtschaftlicher und archivarischer EDV-Anwendungen für die Rundfunkanstalten im Auftrag Dritter. Ferner übernimmt das IVZ die Beratung bei der Planung, Ausrüstung, Organisation, Programmierung und Durchführung elektronischer Datenverarbeitung auch außerhalb des Betriebs dieser Einrichtung (vgl. § 1 Abs. 2 der Verwaltungsvereinbarung vom Januar 2005).

Seit 2004 finden regelmäßig Informationsveranstaltungen für die Datenschutzbeauftragten der beteiligten Anstalten zum Thema „Datenschutz und Datensicherheit“ in Berlin beim IVZ statt. Im Berichtszeitraum gab es derartige Treffen am 9. Juni 2005 und am 22. März 2006. Diese Zusammenarbeit ist deshalb wichtig, weil im IVZ Daten des SR verarbeitet werden, für die das saarländische Recht gilt. In beiden Fällen war die Mitarbeiterin des Referats Datenschutz des SR, Frau Pia Grossmann, anwesend.

Anlässlich der genannten Datenschützertreffen waren folgende Themen relevant:

- Wartungsverträge
- Aktualisierung der Datenschutz-/Datensicherungsmaßnahmen und Arbeitsrichtlinien im IVZ
- IVZ-Strategiepapier 2005 – 2008
- ARD-CN-Sicherheitsgruppe
- Auswertung Penetrationstest im IVZ und weitere Konsequenzen auf Intrusion Detection System (IDS) und Intrusion Prevention (IPS)
- SAP Exchange Infrastructure
- Elster-Verfahren
- BSI-Zertifizierung
- IVZ-Richtlinie für externe Arbeitsplätze
- Präsentation ZEGARD
- Präsentation SAP XI

IV. Datenschutz beim Rundfunkgebühreneinzug

1. Allgemeines

Die Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland, abgekürzt GEZ, ist eine nicht rechtsfähige Verwaltungsgemeinschaft. Sie dient den Rundfunkanstalten als gemeinsames Rechenzentrum für die Abwicklung des Gebühreneinzugs (vgl. § 1 der Verwaltungsvereinbarung „Gebühreneinzugszentrale“ vom 2. Oktober 1992/13. Januar 1993).

Grundlage für die Erhebung von Rundfunkgebühren ist der Rundfunkgebührenstaatsvertrag (RGebStV).

Der Datenschutz bei der GEZ ist einer der Schwerpunkte der Tätigkeit der Datenschutzbeauftragten der Rundfunkanstalten. Die Bearbeitung dieser Beschwerden erfolgt in Zusammenarbeit mit der betrieblichen Datenschutzbeauftragten der GEZ, Frau Kerstin Arens, die mittlerweile von ihrem Kollegen Christian Kruse unterstützt wird.

Die Bedeutung der GEZ bei der zentralen Verarbeitung personenbezogener Daten spiegelt sich in folgenden Zahlen wider:

Ende Dezember 2005 umfasste der dort geführte Rundfunkteilnehmer-Datenbestand rund 39,4 Millionen Teilnehmerkonten mit insgesamt angemeldeten rund 42,5 Millionen Hörfunkgeräten und 36,9 Millionen Fernsehgeräten. Davon waren 39,1 Millionen Hörfunk- und 33,8 Millionen Fernsehgeräte gebührenpflichtig und 3,4 Millionen Hörfunk- und 3,1 Millionen Fernsehgeräte gebührenbefreit.

Im Saarland war die Geräteentwicklung Ende 2005 wie folgt:

Insgesamt waren Ende Dezember 2005 529.499 Hörfunk- und 470.069 Fernsehgeräte angemeldet. Gebührenpflichtig waren 480.803 Hörfunk- und 423.581 Fernsehgeräte. Ganz oder teilweise von der Gebühr befreit waren 48.696 Hörfunk- und 46.488 Fernsehgeräte.

Im Jahr 2006 gibt es in der gesamten Bundesrepublik etwas höhere Zahlen. Die GEZ führte Ende Dezember vergangenen Jahres rund 39,5 Millionen Teilnehmerkonten. Dabei waren rund 42,8 Millionen Hörfunkgeräte und wieder 36,9 Millionen Fernsehgeräte notiert. Gebührenbefreit waren davon 3,5 Millionen Hörfunk- und 3,2 Millionen Fernsehgeräte.

Im Bereich des Saarländischen Rundfunks hat sich dieser Trend nicht ganz durchgesetzt. Hier waren zum 31.12.2006 insgesamt 529.727 Hörfunk- und 467.888 Fernseh-Teilnehmer gemeldet. Auf sie entfielen 485.340 gebührenpflichtige Hörfunk- und 425.833 gebührenpflichtige Fernsehgeräte. Dagegen waren 44.387 Hörfunk- und 42.055 Fernsehgeräte ganz oder teilweise von der Rundfunkgebühr befreit.

Angesichts dieses hohen Teilnehmerbestandes gab es vergleichsweise wenige Beschwerden datenschutzrechtlicher Art, wenn auch eine steigende Tendenz zu

erkennen ist. Bei der GEZ gingen 2005 insgesamt 665 Eingaben von Rundfunkteilnehmern und Anfragen etc. Dritter ein. Auf den SR entfielen lediglich zwei Anfragen. Im Jahr 2006 waren es schon 889 Eingaben bzw. Anfragen, die bei der GEZ eingingen. Immerhin vierzehn davon entfielen auf den SR. Es handelte sich um ein Ersuchen eines Rundfunkteilnehmers um Auskunft über zu seiner Person gespeicherte Daten, sieben Fragen bezüglich der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung, vier Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen, eine Anfrage von einem Finanzamt nach Daten von Rundfunkteilnehmern und eine andere, diesen Fallgruppen nicht zuzuordnende Anfrage. Oftmals geht es den Beschwerdeführern gar nicht um Fragen des Datenschutzes im eigentlichen Sinn, sondern um Inhalte des Rundfunkgebührenstaatsvertrages, die erläutert werden müssen.

2. Neues Befreiungsverfahren

Wie bereits oben in II. c. 1. erwähnt, gibt es seit 1. April 2005 mit § 6 Abs. 2 RGebStV eine Neuregelung zur Rundfunkgebührenbefreiung. In der Praxis bereitet diese erhebliche Probleme und ist zudem datenschutzrechtlich bedenklich.

Der Antragsteller muss nun nach den Vorgaben des Gesetzgebers die Voraussetzungen der Befreiungstatbestände durch Vorlage der Bescheide der Sozialträger im Original oder in beglaubigter Kopie bei der GEZ nachweisen.

Somit müssen die entsprechenden Bescheide z. B. über Arbeitslosengeld II vorgelegt werden, die u. a. auch detaillierte Angaben über die Lebensumstände des Antragstellers oder sogar dritter Personen (z. B. Lebensgefährten) enthalten können und für die GEZ auch tatsächlich nicht von Interesse sind. Es ist indessen eine Frage der Verwaltungspraxis, eine „abgespeckte“ Ausfertigung des jeweils vorzulegenden Bescheids zu erstellen. Mit anderen Worten: nicht der Gesetzgeber oder die GEZ sind gefordert, sondern die Behörden, die sich im Zeitalter des Computers bisher nicht in der Lage sehen, dem Bürger eine um die für die Zwecke der Rundfunkgebührenbefreiung nicht benötigten Daten bereinigte Ausfertigung ihres Bescheides auszuhändigen.

3. Neuer Internetauftritt der GEZ

Unter www.gez.de präsentiert sich die GEZ nun kundenfreundlicher in neuem Gewand. Dabei sind auch die Erläuterungen zum Datenschutz aktualisiert und ergänzt worden. Das Stichwort „Datenschutz“ ist unter neuer Navigation wesentlich schneller auffindbar als zuvor. Über diverse Buttons „Hinweise zum Datenschutz“ kann der interessierte Bürger mit einem Mausklick unmittelbar auf die Erläuterungen zum Datenschutz zugreifen. Das Merkblatt „Datenschutz für Rundfunkteilnehmer“ wird als pdf-Datei zum Ausdruck oder Download bereit gestellt. Gleichfalls werden die Namen und Kontaktdaten der Rundfunkdatenschutzbeauftragten sowie der betrieblichen Datenschutzbeauftragten der GEZ

an leicht auffindbarer Stelle präsentiert, was auf eine Verabredung im AK DSB zurückzuführen ist.

4. DV 2005

Die Umstellung auf das neue DV-System hat Mitte 2005 stattgefunden. Im Vorfeld war eine Arbeitsgruppe „Vorabkontrolle“ unter der Leitung der betrieblichen Datenschutzbeauftragten der GEZ aufgelegt worden, welche die Einführung und Systemumstellung begleitete. Es werden einige Nachbesserungen vorzunehmen sein, auf die nach einer geplanten Überprüfung durch die Rundfunkdatenschutzbeauftragten im kommenden Bericht Bezug genommen werden wird.

5. Rundfunkgebührenbeauftragtendienst
Datenschutzrechtliche Anfragen zum Rundfunkgebührendienst

Im hiesigen Sendegebiet gab es vereinzelte Anfragen von Rundfunkteilnehmern. Zum einen werden sie dem Datenschutzbeauftragten des SR über den Landesdatenschutzbeauftragten zugeleitet, zum andern erreichen sie ihn auf direktem Wege. Dabei bleibt festzuhalten, dass es hier mehr um Erklärung gebührenrechtlicher Gesetzestatbestände als um Datenschutz im engeren Sinn geht. Dabei ging es etwa in einem Fall um die Beschwerde einer Person, die richtigerweise zur Gebührenzahlung trotz Angabe, ihren Fernsehapparat nur zum Ansehen von DVDs zu benutzen, herangezogen worden war. Zuweilen resultieren hieraus Gebührenprozesse vor dem Verwaltungsgericht des Saarlandes.
Daneben erreichen den SR des Öfteren Anfragen nach Auskunft über die bei der GEZ gespeicherten Daten über Rundfunkteilnehmer, die dann selbstverständlich gegeben werden.

6. Prüfung der Gebühreneinzugszentrale durch die Landesdatenschutzbeauftragten von Hessen, Berlin und Brandenburg

Wie berichtet hatten die vorgenannten Landesdatenschutzbeauftragten im September 2004 eine gemeinsame datenschutzrechtliche Kontrolle der GEZ durchgeführt. Durch die Regelung der geteilten Kontrollkompetenz sind nämlich beim Hessischen Rundfunk (hr), Radio Bremen (RB) und dem Rundfunk Berlin Brandenburg (rbb) für den nicht journalistisch-redaktionellen Bereich die entsprechenden Landesdatenschutzbeauftragten zuständig. (Für den journalistisch-redaktionellen Bereich sind es die Rundfunkdatenschutzbeauftragten. In den übrigen Bundesländern liegt die Kontrollkompetenz für die Landesrundfunkanstalten generell bei den Rundfunkdatenschutzbeauftragten.) An dieser Prüfung hatten daher auch einige Rundfunkdatenschutzbeauftragte und andere Mitarbeiter aus den betroffenen Anstalten teilgenommen.

Prüfungsschwerpunkte waren die Organisation der Datensicherheit, der Umfang der Datenverarbeitung im aktiven Teilnehmerkonto, die Verarbeitung der Meldedaten und von Adressdaten aus dem privaten Adresshandel, das Löschungskonzept der GEZ, die Datenverarbeitung im Rahmen der Gebührenbefreiung, durch die Beauftragten und durch externe Dienstleister im Auftrag der GEZ. Besondere Kritikpunkte ergaben sich in puncto Mailing und bei der Auslagerung diverser Arbeiten an externe Firmen.

hr, rbb und RB haben Anfang 2006 in einer ausführlichen gemeinsamen Stellungnahme an die Landesdatenschutzbeauftragten geantwortet und dargelegt, dass viele der Empfehlungen aus dem Prüfbericht übernommen sowie Änderungen umgesetzt oder eingearbeitet werden konnten. Wo das nicht der Fall war, wurden ausführliche Begründungen abgegeben, um so Missverständnisse und Bedenken auszuräumen.

7. Datenschutzverstoß bei einem externen Dienstleister der GEZ

Im November 2005 gab es Hinweise auf einen Datenschutzverstoß bei einem externen Dienstleister der GEZ. Der Vertragspartner der GEZ bzw. der Subunternehmer, der sich mit einer weiteren Firma das Betriebsgelände teilt, war den vertraglich vereinbarten Auflagen zu einer datenschutzgerechten Aufbewahrung und Entsorgung der bis zum Umstieg auf DV 2005 zu bearbeitenden Papierbelege nicht nachgekommen. Der Subunternehmer hatte nicht – wie vertraglich vereinbart – die Papierbelege in verschlossenen Alucontainern auf dem Betriebsgelände gelagert, sondern in verschließbaren, aber dennoch leicht zu öffnenden Plastikcontainern, aus denen Dokumente einfach entnommen werden konnten. Der Subunternehmer hat somit den vertraglichen Vereinbarungen, wonach dafür Sorge zu tragen war, dass die Belege der GEZ für Dritte nicht zugänglich sein dürfen, verletzt. Der unmittelbare Vertragspartner der GEZ, der seinerseits die Einhaltung der vertraglichen Vorgaben garantiert hatte, war somit seinen Kontrollpflichten nicht nachgekommen. Der GEZ-Geschäftsführer hat nach Bekanntwerden des Vorfalls seine Revision mit einer Untersuchung des Vorfalls beauftragt. In einem Gespräch vor Ort unter Beteiligung der Revision der GEZ musste festgestellt werden, dass weder bei einem Subunternehmer noch durch den unmittelbaren Vertragspartner Prüfungen der datenschutzgerechten Aufbewahrung und Entsorgung der GEZ-Belege stattgefunden hatten. Es konnten weder Vernichtungsprotokolle noch sonstige entlastende Unterlagen vorgelegt werden. Die Geschäftsleitung der GEZ hat deren Verwaltungsrat und den AK DSB unmittelbar nach Abschluss der Aufklärungen über die festgestellten Vorgänge und das geplante weitere Vorgehen informiert.

Obwohl seit der Einführung des elektronischen Workflows keine Papierbelege mehr zu den Auftragsdatenverarbeitern gelangen, hat die GEZ beschlossen, einen Aufhebungsvertrag mit Wirkung zum Ende des 1. Quartals 2006 abzuschließen. Dies wurde gegenüber den Alternativen, das Auslaufen des Vertrages zum Jahresende 2006 abzuwarten oder eine fristlose Kündigung auszusprechen, als geeignetes Mittel angesehen. Hierbei spielte vor allem eine Rolle, dass wegen der inzwischen eingeführten papierlosen Bearbeitung kein Verstoß mehr zu erwarten war, dem Risiko einer Klage durch den Dienstleister oder einer seiner Beschäftigten aus dem Weg gegangen wird, der Dienstleister die Arbeits-

verhältnisse mit seinen rund 36 Mitarbeitern abwickeln konnte und die Bearbeitung mit ordentlichen Einarbeitungszeiten auf einen anderen Dienstleister überführt werden konnten.

Verwaltungsrat der GEZ und AK DSB wurden eingehend informiert, letzterer insbesondere über die Sicherstellung des Datenschutzes bis zum Auslaufen des Vertrags.

Als Konsequenz ergibt sich, dass die GEZ künftig im Rahmen der Auftragsdatenverarbeitung keine Verträge mehr schließen wird, bei denen die eigentliche Bearbeitung von einem Subunternehmer durchgeführt wird oder an denen ein Subunternehmer maßgeblich beteiligt ist.

8. Einführung einer sog. NP-Datenbank

Die GEZ hat vor, eine Betriebsstättendatenbank einzuführen, um Gebührenpotential aus dem nicht privaten Teilnehmerumfeld zu gewinnen. Zunächst hatte die GEZ das Projekt NPMARK aufgesetzt, das gegenüber der ursprünglichen Absicht einer Integration in DV 2005 erhebliche Erweiterungen vorsah. Darüber hinaus waren seitens der Gebührenabteilungen vielfältige Anforderungen an die Aufnahme von Daten gestellt worden (z. B. Gründungsdatum einer Gesellschaft, Anzahl der Mitarbeiter), die zuvor aus datenschutzrechtlicher Sicht verworfen worden waren. Das Konzept sah überdies die generelle Verwendung von Anschriften potentieller Teilnehmer für Telefonmarketing sowie die Weitergabe an den Beauftragtendienst der jeweiligen Landesrundfunkanstalt vor.

Dies widersprach den ausdrücklichen Empfehlungen des AK DSB. Es erfolgte am 7. November 2005 eine Präsentation für den AK DSB, dessen Mitglieder (mit Ausnahme der Datenschutzbeauftragten von SWR und NDR) die präsentierte Version der Datenbank für nicht vertretbar hielten. Gründe hierfür waren insbesondere die dauerhafte Speicherung der Daten und deren Umfang. Daraufhin hatte die Geschäftsführung des GEZ ein Gutachten in Auftrag gegeben, das im Ergebnis zu mehr Irritationen führte und nicht die gewünschte Klärung des Sachverhalts zur Folge hatte. Insgesamt hat sich ergeben, dass einige Themenkomplexe unter datenschutzrechtlichen Gesichtspunkten noch einer näheren Prüfung bedurften:

- Dauer der Speicher-/Löschfristen
- Umfang der gespeicherten Daten (insbesondere Geburtsdaten und Kommunikationsadressen der Ein-Personen-Gesellschaften/Freiberufler)
- Verknüpfungen der Daten der NP-Datenbank mit den Daten bereits angemeldeter Teilnehmer
- Weitergabe von Daten (insbesondere der Ein-Personen-Gesellschaften) an den Beauftragtendienst

Eine höchstzulässige Speicherdauer von zwölf Monaten wurde sodann vorgegeben. Für die Speicherung von Namen und Geburtsdaten der Geschäftsführer bzw. Vorstandsmitglieder wurde die Zweckdienlichkeit und Zulässigkeit festgestellt.

Das Fachkonzept der NP-Datenbank wurde demnach überarbeitet, dann hat sich der AK DSB in seiner Herbstsitzung 2006 damit befasst. Zwar gibt es keine grundlegenden Bedenken mehr, aber der Online-Zugriff der Gebühren- bzw. Unterbeauftragten wird als problematisch angesehen. In den weiteren Prüfungen haben sich Unstimmigkeiten hinsichtlich der Umsetzung der geforderten zwölfmonatigen Speicherdauer ergeben. Die diesbezüglichen Beratungen sind noch nicht abgeschlossen.

V. Sitzungen des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und der Deutschen Welle (AK DSB)

Den im Jahr 2005 amtierenden Vorsitzenden des AK DSB, Herrn Prof. Dr. Herb vom SWR, löst seit Januar 2006 Herr Thomas Drescher vom WDR ab.

Im Berichtszeitraum tagte der AK DSB insgesamt fünf Mal:

1. am 10. und 11. März 2005 hier in Saarbrücken,
2. am 13. und 14. Oktober 2005 beim NDR in Hamburg,
3. am 7. November 2005 bei der GEZ in Köln,
4. am 22. und 23. März 2006 beim Deutschlandradio in Berlin,
5. am 21. und 22. September 2006 bei Radio Bremen.

Hierbei wurden die folgenden Themen besprochen:

1. Datenschutzgesetzgebung / Datenschutzpolitik / Rechtsprechung

- Neues TKG
- Entwurf Telemediengesetz
- Entwurf TKÜV
- Novellierung des Signaturgesetzes
- Fortentwicklung der Medienordnung durch ein zukünftiges Telemediengesetz
- Informationsfreiheitsgesetze (IFG) der Länder
- Richtlinien des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zu Änderung der Richtlinie 2002/58/EG
- EuGH-Entscheidung zur Flugdatenweitergabe
- Vorgesehene Änderung beim Melderecht

2. Stellung des Rundfunkdatenschutzbeauftragten

- Zusammenarbeit mit anderen Datenschutzkontrollinstanzen
- Konferenz der staatlichen Datenschützer und deren AK Medien
- Virtuelles Datenschutzbüro
- Prüfung des Unabhängigen Landeszentrums für den Datenschutz (ULD) durch den Landesrechnungshof Schleswig-Holstein
- Veröffentlichung der Tätigkeitsberichte der Rundfunkbeauftragten für den Datenschutz
- Europäische Datenschutzinstitutionen
- Arbeitsgruppe nach Art. 29 EG-Datenschutzrichtlinie
- Europäischer Datenschutzbeauftragter
- Abordnung nationaler Experten zum Europäischen DSB

- EBU/UER
- Zusammenarbeit mit IT-Sicherheitsbeauftragten
- Corporate Identity des AK DSB

3. Datenschutz bei ARD und ZDF

- Datenschutzrechtliche Aspekte von Teleheimarbeit
- Datenschutz und Datensicherheit beim IVZ
- Online-Buchung von Hotels über hotel.de
- Vereinbarung mit BCD Travel (Datenschutzklausel)
- Allgemeine Geschäftsbedingungen für bahn-corporate-online-Kunden
- Code of Conduct zur Behandlung von datenschutzrechtlichen Anfragen, Beschwerden und Auskunftsverlangen
- INFOnline/IVW-Box
- Einrichtung einer unabhängigen Prüfungs- und Beschwerdestelle beim WDR
- ARD-Studie zu den rundfunkbezogenen Stasi-Aktivitäten
- Einsatz von Content-, Http- und URL-Filtern
- Cookies und Web-Controlling bei ard.de
- Kopierer mit Festplatten/ Datenschutz bei digitalen Kopiergeräten
- E-Mail-Bearbeitung bei Abwesenheiten
- Datenschutzprüfung ZfP
- Datenschutzhinweis in FESAD
- Missbräuchliche Nutzung von Presseausweisen
- mySAP.ERP 2005 – Auswertung der persönlichen SAP-Nutzung
- Reisekostenabrechnung mit SAP
- Verarbeitung personenbezogener Daten in Auslandsstudios
- Elektronische Bewerbung
- Drehgenehmigungsverträge
- Archivierung
- Vertraulichkeitserklärung für freie Mitarbeiterinnen und Mitarbeiter
- Aufzeichnung von Telefongesprächen
- Einzelverbindungsnachweis
- VPN-Zugänge
- T-Online-Verträge
- Geplante Grundverschlüsselung bei Astra
- Wirtschaftsjournalisten als Insider (Vertraulichkeitserklärungen)
- Orchesterverwaltungssystem OPAS

4. Rundfunkteilnehmerdatenschutz

- Prüfbericht der staatlichen Landesdatenschutzbeauftragten über die Datenverarbeitung bei der GEZ am 21.-23.09.2004 und Stellungnahme dazu

- Datenschutzrechtliche Prüfung des Projekts DV 2005
- Datenschutzrechtliche Kontrolle von Beauftragten
- Neues Befreiungsverfahren Rundfunkgebühr
- Datenschutzrechtliche Gestaltung des Befreiungsantrags
- Elektronisches Formular für Befreiungsantrag
- Weitergabe von Mailingadressen von Kapitalgesellschaften an BAs
- GEZ-Mailing
- 8. Rundfunkänderungsstaatsvertrag - § 8 Abs. 4 RGebStV (neu)
- Rechtswidriges Jugendlichenmailing
- Neufassung der Richtlinien für den Datenschutz der GEZ
- Verarbeitung personenbezogener Daten im Zusammenhang mit der Befreiung von der Rundfunkgebührenpflicht
- AG Musterschreiben
- Unternehmensbezogene Datenschutzinformation
- Internetseiten gegen die GEZ
- NP-Datenbank
- BDONAB
- Feststellung eines datenschutzrechtlichen Verstoßes bei einem externen Dienstleister der GEZ
- Datenerhebung bei Dritten durch die Rundfunkgebührenbeauftragten
- Historie-Löschungskonzept
- Unterlagenaushändigung durch die GEZ an die Landesbeauftragten für den Datenschutz
- LG Darmstadt; Speicherung von Verkehrsdaten
- Auftragsdatenverarbeitung
- Ad-hoc-AG Gebühreneinzugsordnung (GEORG)

VI. Ausblick

Der Rundfunkgebühreneinzug durch die GEZ ist – bedingt durch eine verstärkte Presseberichterstattung – im Berichtszeitraum noch stärker als bisher in den Fokus der Tätigkeit des Rundfunkdatenschutzbeauftragten geraten.

Bezogen auf die Anzahl der angemeldeten Rundfunkempfangsgeräte liegt die absolute Anzahl der zu bearbeitenden Auskunftsersuchen und Beschwerden zwar noch im Nullkommanull-Promillebereich, der Anstieg ist indessen signifikant.

Dabei sind tatsächliche oder vermeintliche Verstöße gegen datenschutzrechtliche Bestimmungen – jedenfalls noch – regelmäßig das Vehikel, nicht aber der Grund für die Befassung des Rundfunkdatenschutzbeauftragten. Im Kern ist die Steigerung einerseits durch eine abnehmende Akzeptanz der Gebührenfinanzierung des öffentlichrechtlichen Rundfunks verursacht; zu einem anderen Teil in der Verunsicherung der Bürger. Es sind – wie gezeigt – z. T. gezielte Fehlinformationen über die Gebührenpflicht, die insoweit einen hohen Nachfragebedarf auslösen.

Es ist aber auch das Unvermögen einzelner Behörden, Bescheidsexemplare so auszufertigen, dass sie ausschließlich die Daten (bzw. Informationen) enthalten, die die GEZ zur Feststellung der Befreiungsvoraussetzungen benötigt. Insoweit sind es nicht der von einzelnen staatlichen Datenschutzbeauftragten angerufene Gesetzgeber oder die oft als „Datenkrake“ titulierte GEZ, die sich den Grundgedanken des Datenschutzes verschließen, sondern die Behörden, die die Bescheide erstellen, die Voraussetzung für eine Befreiung von der Rundfunkgebührenpflicht sind.

Das ist im Gesetzesvollzug durch die Landesrundfunkanstalten (bzw. durch die GEZ) wenig hilfreich und im Umgang der Behörden mit ihrem Klientel wenig bürgernah, wird aber zusehens zu einer Belastung für die Rundfunkanstalten, denen die Versäumnisse der Behörden zugerechnet werden. Deshalb wäre es gewiss nicht ungeschickt, wenn der Gesetz- oder Verordnungsgeber vorschriebe, dass die Behörden mit dem Erlass etwa des ALG-II-Bescheides dem Antragsteller zugleich eine allein für Zwecke der Rundfunkgebührenbefreiung geeignete Ausfertigung dieses Bescheides an die Hand zu geben.

Sorge bereitet indessen auch die beabsichtigte Vorratsdatenspeicherung, die mit der Abwehr terroristischer Bedrohung einhergeht und noch verstärkt einhergehen soll. Aktuell bereitet insbesondere die vorgesehene Neuregelung der Telekommunikationsüberwachung Besorgnis. Die im Gesetzentwurf der Bundesregierung beabsichtigte Einführung verdachtsloser Vorratsdatenspeicherung, die keine Ausnahmetatbestände für Berufsgeheimnisträger, wie unsere Journalisten, vorsieht, stört die auf Vertrauen basierende Beziehung zwischen Journalist und Informant empfindlich. Dass damit ein seriöser, investigativer Journalismus, der auf eine vor äußeren Eingriffen geschützte Informationsbeschaffung angewiesen ist, im Kern getroffen wird, bedarf keiner weitern Ausführungen.

Ohne Informantenschutz und Wahrung des Redaktionsgeheimnisses ist das was die Verfasser unseres Grundgesetzes als freie Presse- und Rundfunkberichterstattung im Sinn hatten, nicht zu gewährleisten.

Saarbrücken, den 5. September 2007

Bernd Radeck
Der Datenschutzbeauftragte

Anlage

Dienstanweisung zum Schutz personenbezogener Daten im SR (Dienstanweisung Datenschutz)

Vom 21.3.2005

1. Zielsetzung

Jeder Mitarbeiter des SR hat im Zusammenhang mit seiner dienstlichen Tätigkeit Zugang zu und Umgang mit personenbezogenen Daten anderer. Die personenbezogenen Daten jedes Mitarbeiters des SR werden an verschiedenen Stellen des Hauses verarbeitet. Der sorgfältige, ordnungsgemäße Umgang mit allen personenbezogenen Daten, sei es im Rahmen der schriftlichen oder fernmündlichen Korrespondenz, in der Aktenführung oder in der elektronischen Verarbeitung personenbezogener Daten, liegt daher im Interesse jeder und jedes einzelnen.
Ziel des Datenschutzes ist es, das Recht des einzelnen zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Die vorliegende Dienstanweisung dient der praktischen Umsetzung der für den Saarländischen Rundfunk maßgeblichen datenschutzrechtlichen Vorschriften. Diese ergeben sich vor allem aus § 11 Saarländisches Mediengesetz (SMG) in Verbindung mit dem Saarländischen Datenschutzgesetz (SDSG).

2. Begriffsbestimmung

2.1 Personenbezogene Daten

sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Dazu zählen z. B. Name, Anschrift, Telefon- oder Telefaxnummern, Geburtsdatum, Personal- oder Rundfunkteilnehmernummer, Gehaltsdaten, Arbeitszeiten usw.

2.2 Verarbeitung personenbezogener Daten

ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten, sofern sie gespeichert oder zur Speicherung vorgesehen sind, und zwar unabhängig davon, ob dies in Papierform (Akten, Karteien) oder automatisiert (EDV) geschieht.

2.3 Befugte

sind Personen, zu deren dienstlichen Aufgaben die Verarbeitung personenbezogener Daten im jeweils erforderlichen Umfang gehört. Unbefugt können daher auch berechtigte Nutzer sein, die bspw. andere oder mehr personenbezogene Daten verarbeiten als dienstlich veranlasst ist, diese Daten länger als dienstlich erforderlich speichern, nicht-berechtigten Dritten Kenntnis verschaffen usw.

2.4 Verarbeitende Stelle

ist im Außenverhältnis zu Dritten der SR insgesamt, im Innenverhältnis der/die jeweils zuständige Fachbereich bzw. Programmgruppe. Die persönliche Verantwortlichkeit jedes Mitarbeiters für die ordnungsgemäße Verarbeitung personenbezogener Daten bleibt hiervon unberührt.

2.5 Maßnahmen zur Datensicherung

sind alle technischen und organisatorischen Maßnahmen, die die Nutzer ergreifen müssen, um die Integrität, Vertraulichkeit und Verfügbarkeit personenbezogener Daten zu sichern. Hierzu gehört neben den unten in Textziffer 5 genannten Vorkehrungen die technische Sicherung elektronisch verarbeiteter personenbezogener Daten durch die regelmäßige Herstellung von Sicherungskopien.

3. Zulässigkeit der Verarbeitung personenbezogener Daten

3.1 Grundsatz

Die Verarbeitung personenbezogener Daten ist verboten, es sei denn, die oder der Betroffene hat eingewilligt oder eine Rechtsvorschrift gestattet sie. Dabei kann es sich um eine Erlaubnisvorschrift des SDSG, aber auch um sonstige gesetzliche, tarifvertragliche oder hausinterne Bestimmungen (z. B. Dienstvereinbarungen oder Dienstanweisungen) handeln. Stets muss die Verarbeitung personenbezogener Daten überdies zur Erfüllung der Aufgaben der verarbeitenden Stelle auch tatsächlich erforderlich sein und sie darf nur den Zwecken dienen, für die die Daten erhoben bzw. für die sie erstmals gespeichert wurden.

3.2 Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken (Medienprivileg)

Soweit personenbezogene Daten zu journalistisch-redaktionellen Zwecken des SR verarbeitet werden, ist grundsätzlich weder die Einwilligung der Betroffenen noch eine spezielle Erlaubnisnorm erforderlich. Auch die sonstigen Einschränkungen des Datenschutzrechts gelten nicht; die Vorschriften der Textziffern 5 bis 7 dieser Dienstanweisung bleiben allerdings unberührt. Die Zulässigkeit der Verarbeitung personenbezogener Daten ergibt sich aus einer Abwägung zwischen dem Grundrecht der Rundfunkfreiheit (Art. 5 GG) und den Schutzrechten der Betroffenen (insbesondere dem Allgemeinen Persönlichkeitsrecht, Art. 2 GG, der Religionsfreiheit, Art. 4 GG, der Meinungsfreiheit, Art. 5 GG und der Berufsfreiheit, Art. 12 GG).

3.3 Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis

Daten von Bewerbern, Volontären, Hospitanten, Praktikanten, Auszubildenden, Aushilfen und von fest angestellten und freien Mitarbeitern dürfen nur verarbeitet werden, soweit dies erforderlich ist, um das Beschäftigungsverhältnis einzugehen, durchzuführen, zu beendigen oder abzuwickeln, oder um organisatorische, personelle oder soziale Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes durchzuführen, oder soweit eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

3.4 Gesundheitsdaten

Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz der betroffenen Beschäftigten dient.

3.5 Verhaltens- und Leistungskontrolle

Soweit Beschäftigtendaten im Rahmen der Maßnahmen zur Datensicherung (s. unten Textziffer 5) gespeichert werden, dürfen sie nicht zu anderen Zwecken, insbesondere nicht zu Zwecken der Verhaltens- oder Leistungskontrolle, genutzt werden.

4. Übermittlung, Weitergabe

Gespeicherte oder durch Verarbeitung personenbezogener Daten gewonnene Daten dürfen grundsätzlich nicht an Dritte weitergegeben oder zum Abruf bereitgehalten werden (Datenübermittlung). "Dritte" sind dabei nur solche Personen und Stellen, die nicht im SR oder in seinem Auftrag tätig sind. Im übrigen richtet sich die Zulässigkeit der Datenübermittlung nach den Vorschriften des § 11 Abs. 4 SMG in Verbindung mit den §§ 13 ff. SDSG sowie § 11 Abs. 5 SMG.
Gespeicherte oder durch Verarbeitung personenbezogener Daten gewonnene Daten dürfen außerdem grundsätzlich nicht Unbefugten zur Kenntnis gegeben werden (Weitergabe). "Unbefugt" ist jeder, der die Daten nicht aus dienstlichen oder sonstigen Gründen zulässigerweise verarbeiten darf.

5. Datensicherung

5.1 Grundsatz

Technische und organisatorische Maßnahmen im jeweils erforderlichen Umfang haben dem Ziel zu dienen, sicher zu stellen, dass personenbezogene Daten nur in zulässiger Weise verarbeitet werden. "Erforderlich" sind Maßnahmen zur Datensicherung, wenn ihr Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht. Je sensibler die Daten also sind, desto vertraulicher müssen sie behandelt und desto strenger gegen Missbrauch gesichert werden.

5.2 Datensicherung bei Karteien und Akten

5.2.1 Aufbewahrung

Alle Unterlagen mit schutzwürdigen personenbezogenen Daten sind gegen unbefugte Einsichtnahme oder Entwendung zu schützen. Vor Verlassen des Arbeitsplatzes müssen sie angemessen gesichert, d. h. verschlossen aufbewahrt werden. Schlüssel dürfen nicht frei zugänglich, sondern müssen ihrerseits gesichert verwahrt werden.

5.2.2 Nutzung

Dienstliche Unterlagen mit personenbezogenen Daten dürfen nur für dienstliche Zwecke genutzt und Dritten innerhalb oder außerhalb des Hauses auch nur insoweit zur Kenntnis gebracht bzw. zugänglich gemacht werden.

5.2.3 Versand vertraulicher Unterlagen, insbesondere Telefax

Vertrauliche Unterlagen sind, soweit sie nicht persönlich zugestellt werden, im fest verschlossenen Umschlag so zu versenden, dass personenbezogene Daten nur im unvermeidbaren Umfang erkennbar sind.
Telefaxgeräte sind so aufzustellen, dass Unbefugte regelmäßig keine Kenntnis vom Inhalt eingehender oder übertragener Telefax-Schreiben erhalten können.
Die dem absendenden Gerät vom empfangenden Gerät übermittelte Kennung ist vom Absender unverzüglich zu überprüfen. Bei Wählfehlern hat er die Verbindung unverzüglich abzubrechen.
Vor der Versendung vertraulicher Daten per Telefax soll der Empfänger über den Zeitpunkt der Übermittlung unterrichtet und sichergestellt werden, dass Unbefugte keine Einsicht erlangen können. Besonders sensible Daten, insbesondere Sozial-, Steuer- und Gesundheitsdaten sollen grundsätzlich nicht per Telefax versandt werden.
Für die Datenübermittlung auf elektronischem Wege (insbesondere e-Mail) gelten diese Grundsätze entsprechend.

5.2.4 Vernichtung
Für dienstliche Zwecke nicht mehr benötigte Unterlagen mit personenbezogenen Daten sind grundsätzlich qualifiziert zu vernichten. Die Vernichtung größerer Mengen übernimmt die Hausverwaltung.

5.3 Datensicherung bei automatisierten Verfahren
5.3.1 Einrichtung und Betrieb automatisierter Verfahren
Für dienstliche Zwecke darf ausschließlich solche Hard- und Software eingesetzt und genutzt werden, die von der für Informationstechnologie zuständige Organisationseinheit(*) geprüft und im Rahmen des hierfür vorgesehenen Verfahrens genehmigt worden ist. Der Einsatz privater Hardware für dienstliche Zwecke im SR und die Verwendung privater Software auf SR-eigenen EDV-Anlagen ist verboten; Textziffer 6.2 bleibt unberührt.

(*) Fachbereich IT in der Verwaltungs- und Betriebsdirektion

Dienstlich genutzte Datenträger dürfen auf externen EDV-Anlagen nur eingesetzt werden, wenn dies betrieblich zwingend erforderlich und gewährleistet ist, dass hierdurch die Sicherheit der SR-eigenen EDV-Anlagen, beispielsweise durch die Übertragung von Viren und dergleichen, nicht gefährdet ist. Entsprechendes gilt für die Nutzung externer Datenträger in SR-eigenen EDV-Anlagen.

5.3.2 Passwortschutz
Grundsätzlich soll der Zugriff auf automatisierte Anwendungen durch ein Passwort geschützt werden. Dieses sollte eine Mindestlänge von sechs Stellen haben und ausschließlich dem Nutzer bekannt sein; es darf daher insbesondere nicht an einer für andere einsehbaren Stelle notiert oder aufbewahrt werden. Eine von anderen durchschaubare Beziehung zum Anwender (Vor- oder Nachname u. dgl.) ist ebenso zu vermeiden wie die Eingabe von Trivialkombinationen (z. B. 4711, 12345... oder andere nebeneinander liegende Tasten); empfehlenswert sind alphanumerische (Buchstaben-/Zahlen-) Kombinationen.
Das Passwort soll, auch soweit dies nicht bereits systemseitig verlangt wird, in angemessenen Zeitabständen durch ein bisher nicht verwendetes ersetzt werden.
Es ist grundsätzlich nicht zulässig, unter einem fremden Passwort zu arbeiten.

5.3.3 Sicherung von Laufwerken und Datenträgern
Disketten- und sonstige Speichermedien (z. B. SD-Karten oder USB-Sticks) sind, soweit technisch möglich, verschlossen zu halten. Disketten, Ausdrucke und andere Datenträger sowie Schlüssel sind gesichert zu verwahren.

5.3.4 Löschung
Der auf EDV-Anlagen gespeicherte Datenbestand ist durch den jeweiligen Nutzer regelmäßig daraufhin zu überprüfen, ob er für dienstliche Zwecke noch erforderlich ist. Anderenfalls muss er gelöscht oder für den aktuellen Zugriff bzw. die weitere Verarbeitung gesperrt werden.

6. Einsatz portabler Computer (Laptops, Notebooks usw.) und Fernzugriff
6.1 Allgemeine Nutzungsbestimmungen
Portable Computer dürfen nur von den jeweils autorisierten Personen genutzt werden. Sie sind gegen Diebstahl besonders zu sichern und dürfen insbesondere nicht unbe-

aufsichtigt in Fahrzeugen zurückgelassen werden. Im übrigen gelten die Vorschriften der Textziffern 5.3.2 bis 5.3.4 entsprechend.

6.2 Einsatz privater Hardware

Soweit – insbesondere durch freie Mitarbeiter – private portable Computer für Zwecke des SR eingesetzt werden, ist sicherzustellen, dass die Nutzer die Sicherheitsbestimmungen des SR einhalten und sich der Kontrolle des Datenschutzbeauftragten des SR unterwerfen.

6.3 Sicherheitsüberprüfung

In regelmäßigen Abständen, in jedem Falle aber vor dem Anschluss an andere EDV-Anlagen des SR ist eine Überprüfung portabler Computer auf Manipulation, Viren und dergleichen durch die für Informationstechnologie zuständige Organisationseinheit(*) zu veranlassen. Bei Unregelmäßigkeiten ist die für Informationstechnologie zuständige Organisationseinheit(*) unverzüglich zu benachrichtigen.

6.4 Fernzugriff

Der Zugriff auf das Intranet des SR über Weitverkehrsverbindungen (Fernzugriff) darf nur durch autorisierte Personen unter Einsatz von Verfahren sowie Hard- und Software, die zuvor durch die für Informationstechnologie zuständige Organisationseinheit(*) freigegeben wurden, erfolgen. Die Genehmigung von Fernzugriffen auf das Intranet des SR zum Zwecke der Wartung durch Dritte bedarf der vorherigen Erklärung des Dritten, die Bestimmungen des Datenschutzes einzuhalten. Die Erklärung bedarf der Schriftform.
Der Einsatz von Computern, die mit einer Weitverkehrsverbindungstechnik (DSL, ISDN, Modem usw.) ausgestatten sind, im SR-Intranet ist auf das dienstlich notwendige Minimum einzuschränken und bedarf der Installation geeigneter Schutzmaßnahmen, die durch die für Informationstechnologie zuständige Organisationseinheit(*) vorgegeben werden.

7. Allgemeine Rechte und Pflichten

7.1 Datengeheimnis, Vertraulichkeit

Es ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben oder zugänglich zu machen.
Alle Mitarbeiter des SR sind verpflichtet, personenbezogene Daten, von denen sie durch ihre Tätigkeit für den SR Kenntnis erlangen, vertraulich zu behandeln. Dies gilt auch über die Dauer der Beschäftigung für den SR hinaus.

7.2 Auskunftsersuchen, Presserechtliche Erklärungen

Behördliche, gerichtliche oder sonstige Ersuchen auf Auskunft über die im SR bzw. in seinem Auftrag verarbeiteten personenbezogenen Daten dürfen nur nach Maßgabe einer Rechtsvorschrift oder mit Einwilligung der oder des Betroffenen beantwortet werden. Sowohl für das Auskunftsersuchen wie auch für die Beantwortung gilt das Schriftformerfordernis. In Zweifelsfällen über die Berechtigung und die Angemessenheit der Datenübermittlung ist der Dienstvorgesetzte und gegebenenfalls der Datenschutzbeauftragte einzuschalten.
Führt die journalistisch-redaktionelle Verwendung personenbezogener Daten zu Gegendarstellungen der Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

7.3 Mitteilungspflicht
Mängel oder Auffälligkeiten im Datenverarbeitungs- oder -sicherungssystem sind unverzüglich der oder dem Vorgesetzten sowie gegebenenfalls dem Datenschutzbeauftragten zu melden.

7.4 Anrufung des Datenschutzbeauftragten
Jeder Mitarbeiter hat das Recht, sich jederzeit unmittelbar an den Datenschutzbeauftragten zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den SR oder die in dessen Auftrag tätig werdenden Dritten in seinen schutzwürdigen Interessen verletzt worden zu sein. Aus der Wahrnehmung dieses Rechts dürfen dem Mitarbeiter keine Nachteile entstehen.

7.5 Sonstige Rechte
Die sonstigen Rechte der Betroffenen, insbesondere auf Auskunft über Art und Umfang gespeicherter Daten, Berichtigung usw. ergeben sich aus den für den SR maßgeblichen Vorschriften des Saarländischen Datenschutzgesetzes.

8. Schlussvorschrift
Soweit in dieser Dienstanweisung geschlechtsbezogene personenbezogene Bezeichnungen verwendetet werden, gelten sie für Frauen in der weiblichen, für Männer in der männlichen Sprachform.
Diese Dienstanweisung tritt am 4. April 2005 in Kraft.

Anlage zur Dienstanweisung zum Schutz personenbezogener Daten im SR (Dienstanweisung Datenschutz)

Regeln zum sicheren Umgang mit vernetzten Systemen

1. Niemand außer dir darf dein Passwort wissen!

2. Sei dir bewusst: Du allein bist verantwortlich für alles, was unter Nutzung deiner Zugangsberechtigung gemacht und veranlasst wird.

3. Verständige bei Verdacht auf Zugriffsverstöße sofort deinen Administrator!

4. Schalte bei Verlassen des Arbeitsplatzes unbedingt den aktiven Bildschirmschoner ein!

5. Nutze deinen Arbeitsplatz-PC ausschließlich für dienstliche Zwecke!

6. Hände weg von nichtautorisierter Hard- und Software bei der Arbeit mit dem Arbeitsplatz-PC!

7. Vermeide "Schmuddelkram" im Internet!

8. Denke daran, dass E-Mails genauso vertraulich wie Postkarten sind.

9. Öffne niemals E-Mail-Anlagen ("Attachements") von Absendern, die du nicht kennst, und lösche Hoaxes (vermeintliche Virenwarnungen) und Kettenbriefe sofort!

10. Sei stets (selbst-)kritisch im Umgang mit einem vernetzten PC!