WDR

# 21. Tätigkeitsbericht des Datenschutzbeauftragten des Westdeutschen Rundfunks Köln

# Inhalt


**Vorbemerkung** 4

**A. Aufgaben des Datenschutzbeauftragten** 5

**B. Entwicklung des Datenschutzrechts** 6

1. Zusammenfassende Würdigung 6
2. Europa 6
3. Bundesrecht 6
   - 3.1 Mehr Befugnisse für das Bundeskriminalamt (BKA-Gesetz) 6
   - 3.2 Sicherheit in der Informationstechnik (BSI-Gesetz) 7
   - 3.3 Drei neue BDSG-Novellen im Jahr 2009 7
   - 3.4 Arbeitsmedizinische Vorsorgeuntersuchungen 8
   - 3.5 Volkszählung 2011 (Zensusgesetz) 8
   - 3.6 ELENA – der elektronische Entgeltnachweis 8
   - 3.7 Landesgesetzgebung – Rundfunkrechtliche Staatsverträge 9
   - 3.8 Weitere Gesetzesvorhaben und Entwicklungen 9

**C. Datenschutz im WDR** 11

1. Online-Aktivitäten 11
   - 1.1 Datenschutzrichtlinie für soziale Netzwerke im Rundfunkbereich 11
   - 1.2 Jugendliche und Datenschutz 11
   - 1.3 Datenumfang bei der Nutzung von Online-Angeboten 11
   - 1.4 Gewinnspiele und der Umgang mit Adressen der Hörer/-innen und Zuschauer/-innen 12
2. Datenschutz in den SAP-gesteuerten Modulen (FI, CO, COGHOS, MM usw.) 13
   - 2.1 Ziel des WDR-Berechtigungskonzepts 13
   - 2.2 Sicherstellung der Revisionsfähigkeit des WDR-Berechtigungskonzepts 14
3. Absicherung von Produktionsgewerken vor Bedrohungen aus dem Internet 14
   - 3.1 Besondere Gefährdung der Produktions-IT 14
   - 3.2 Schutzsoftware nur beschränkt wirksam 14
   - 3.3 Abhilfe nicht immer schnell möglich 14
   - 3.4 Absichern des Internet-Zugriffs durch Hinweis-Fenster 14
   - 3.5 Nutzung nach Authentifizierung mit der persönlichen Kennung 14
   - 3.6 Funktion nur nach Anforderung durch Systembetreiber 15
   - 3.7 Anfälligkeit gegenüber Bedrohungen aus dem Internet wird minimiert 15
   - 3.8 Log-Dateien 15
   - 3.9 Datenschutz 15

**D. Datenschutz beim Rundfunkgebühreneinzug** 16

1. Gegenwärtige Situation 16
   - 1.1 GEZ – Gebühreneinzugszentrale der öffentlich-rechtlichen Landesrundfunkanstalten 16
   - 1.2 Datenbestand bei der GEZ und beim WDR 16
   - 1.3 Anfragen und Auskunftsersuchen 16
   - 1.4 Mailing – ein Dauerbrenner 17
2. Vorbereitung der Umsetzung der Neuregelungen im Rundfunkbeitragsstaatsvertrag 18

**Schlussbemerkung** 19

# Vorbemerkung

Der Beauftragte für den Datenschutz des WDR hat dem Rundfunkrat alle zwei Jahre einen Bericht über seine Tätigkeit zu erstatten (§ 53 Abs. 7 WDR-Gesetz). Der Bericht ist im Online-Angebot des WDR zu veröffentlichen.

Dieser Verpflichtung komme ich hiermit für den Zeitraum 2009/2010 nach.

# A Aufgaben des Datenschutzbeauftragten

Nach § 53 Abs. 1 WDR-Gesetz tritt der/die Beauftragte für den Datenschutz beim WDR an die Stelle des oder der Landesbeauftragten für den Datenschutz und Informationsfreiheit, allerdings nur insoweit, als es um datenschutzrechtliche Fragen geht.

Der Beauftragte für den Datenschutz beim WDR nimmt ausdrücklich nicht die Aufgaben eines Beauftragten für Informationsfreiheit wahr.

Die Aufgabenstellung umfasst nach § 53 Abs. 2 Satz 1 WDR-Gesetz die Einhaltung der Datenschutzvorschriften des WDR-Gesetzes, des Datenschutzgesetzes Nordrhein-Westfalen und anderer Vorschriften für den Datenschutz bei der gesamten Tätigkeit des WDR.

Schwerpunkte meiner Arbeit bilden nach wie vor Kontroll- und Informationsbesuche in den verschiedenen Bereichen des Hauses einschließlich der GEZ. Hierbei steht die Beratung im Vordergrund. Bei festgestellten Mängeln und Defiziten hat Bereitschaft zur Abhilfe bestanden und meine Verbesserungsvorschläge wurden aufgenommen.

Festzustellen ist auch, dass die Digitalisierung und »Computerisierung« beim WDR nicht nur im Verwaltungsbereich voranschreitet, sondern mit steigender Tendenz auch die Programm- und Produktionsbereiche erfasst. Hierbei ist festzustellen, dass zunehmend die Einbindung des Datenschutzbeauftragten im Rahmen laufender Projekte oder Prozesse oder aber auch aufgrund entsprechender Nachfragen seitens der Fachbereiche des Hauses oder des Personalrates in erfreulichem Maße sichergestellt ist.

Dementsprechend bin ich verstärkt auch bei der Einführung WDR-weiter Maßnahmen mit datenschutzrechtlichen Auswirkungen beteiligt worden.

Außerdem findet auch in regelmäßigen Abständen ein Informations- und Erfahrungsaustausch mit dem Personalrat statt.

Die Informationen, die ich als Bürgerservice und als Hilfestellung auch über das Internetangebot des WDR eingestellt habe, sind dort weiterhin abrufbar. Hier wird in Abstimmung mit den zuständigen Fachbereichen des Hauses ständig daran gearbeitet, diese Informationen zu aktualisieren und so zu gestalten, dass sie bei den Nutzerinnen und Nutzern auf Interesse stoßen.

Auch das Intranetangebot des Datenschutzbeauftragten des WDR steht weiterhin für die Mitarbeiter/innen bereit und wird ständig aktualisiert und angepasst.

Nach § 11 Abs. 1 WDR-Gesetz hat jeder das Recht, sich unmittelbar an den Datenschutzbeauftragten des WDR zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den WDR in seinen schutzwürdigen Belangen verletzt worden zu sein. In erster Linie machen hiervon Rundfunkteilnehmer/innen und auch Mitarbeiter/innen Gebrauch, die sich wie andere Bürger auch schriftlich, telefonisch oder per E-Mail an mich wenden. Es geht dabei – wie in den vergangenen Jahren – nicht immer nur um datenschutzrechtliche Beschwerden. Vielfach werde ich auch um Auskünfte im Zusammenhang mit dem Rundfunkgebühreneinzug, der Behandlung von Teilnehmerpost und unverlangten Werbesendungen gebeten.

Der Vollständigkeit halber sei darauf hingewiesen, dass ich entsprechend der einschlägigen gesetzlichen Regelung neben meiner Tätigkeit als Datenschutzbeauftragter auch noch Aufgaben im Justiziariat des WDR wahrnehme.

# B Entwicklung des Datenschutzrechts

## 1. Zusammenfassende Würdigung

Das Datenschutzbewusstsein in Deutschland hat wieder zugenommen. Zahlreiche Datenskandale in der Wirtschaft bescherten dem Datenschutz, also dem Persönlichkeitsrecht des Einzelnen, eine Renaissance. Beim WDR indessen gab es auch in den letzten Jahren keine Skandale und keine Vorkommnisse, die zu einer Beanstandung und damit förmlichen Befassung des Rundfunkrates (§ 53 Abs. 3 WDR-Gesetz) Anlass geboten hätten.

Dieser 21. Bericht zeigt auch, dass sich die autonome Kontrolle beim WDR – ohne staatliche Einflussnahme – bewährt hat und die Persönlichkeitsrechte der Rundfunkteilnehmer, der Nutzer der EDV-Programme und der vielen festen und freien Mitarbeiter geschützt werden. Diesen hohen Standard könnten externe Kontrollen etwa durch die Landesdatenschutzbeauftragten bei Weitem nicht sicherstellen. Die Entwicklungslinien der vergangenen Jahre setzten sich auch weiterhin fort:

- Der Gesetzgeber will Probleme mit Datensammlungen und -überwachungen lösen und produziert immer neue freiheitsbeschränkende Gesetze.
- Ein Dauerbrenner ist nach wie vor der Datenschutz im Bereich des Rundfunkgebühreneinzuges. Diese Tendenz dürfte auch im Falle der Umstellung des Systems der Rundfunkfinanzierung von einer geräteabhängigen Gebühr auf einen geräteunabhängigen Haushalts- und Betriebsstättenbeitrag zunächst nicht abnehmen, da insbesondere in der Übergangsphase auch mit einer Verunsicherung der Bürgerinnen und Bürger über den Schutz ihrer persönlichen Daten im Zusammenhang mit der Umstellung des Rundfunkgebühreneinzugs auszugehen ist.

## 2. Europa

Die Tätigkeit der Europäischen Gemeinschaften bzw. der Europäischen Union beeinflusste zunehmend die Gesetzgebung und die Rechtswirklichkeit in der Bundesrepublik. Dies gilt auch für das Datenschutzrecht. So wurde seit meinem letzten Bericht u. a. das Bundesdatenschutzgesetz deutlich verändert. Gegenwärtig findet auch eine Diskussion über die Modernisierung des Datenschutzrechts in Europa unter Einbeziehung einer möglichen Novellierung der Europäischen Datenschutzrichtlinie statt. Hier gibt es neben den Aktivitäten der Kommission auch solche des Europäischen Parlaments, das sich der Frage des Datenschutzrechts auch zunehmend annimmt. Auch ich habe gegenüber der Kommission zu Fragen der Modernisierung des Datenschutzrechts im Bereich des Rundfunks Stellung genommen.

## 3. Bundesrecht

In den letzten Jahren wurden wieder zahlreiche Gesetze – vor allem im Sicherheitsbereich – erlassen, die in großem Umfang auch das informationelle Selbstbestimmungsrecht des Einzelnen belasten. In verschiedenen Fällen (Vorratsdatenspeicherung) konnte erst durch Entscheidungen des Bundesverfassungsgerichts eine ausgewogene Anwendbarkeit entsprechender Regelungen sichergestellt werden.

### 3.1 Mehr Befugnisse für das Bundeskriminalamt (BKA-Gesetz)

Staatliche Organe können zur Gefahrenabwehr oder auch zur Strafverfolgung tätig werden. Nachdem in der Strafprozessordnung schon umfangreiche Befugnisse zur Strafverfolgung enthalten sind, wurden die Befugnisse für die Gefahrenabwehr noch weiter ausgedehnt. So sind mit Gesetz vom 25. Dezember 2008 (BGBl Seite 3083) die Möglichkeiten des Bundeskriminalamtes (BKA) erheblich ausgeweitet worden. Ein neuer Unterabschnitt regelt in seinen 20 Paragrafen von § 20 a bis § 20 t die verschiedensten Maßnahmen. So dürfen z. B. nach § 20 h BKA-Gesetz heimliche Ton- und Bildaufnahmen auch in Wohnungen gemacht werden und mit § 20 k BKA-Gesetz dürfen verdeckte Eingriffe in informationstechnische Systeme vorgenommen werden, also darf z. B. mithilfe eines sog. Trojaners in private Computer eingedrungen werden.

Mit den entsprechenden Regelungen wurde das BKA im Bereich der Gefahrenabwehr im Hinblick auf den »Internationalen Terrorismus« bei seinen Befugnissen den Polizeibehörden der Bundesländer gleichgestellt. Einer vorherigen Änderung des Art. 13 GG bedurfte es nach Ansicht des Bundesjustizministeriums nicht. Vielmehr gestatte Art. 13 Abs. 4 GG derartige Maßnahmen. Eine Online-Durchsuchung stellt im Übrigen nach der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 keinen Eingriff in Art. 13 GG dar. Allerdings stehen alle Befugnisse des BKA mit hoher Eingriffstiefe unter Richtervorbehalt.

Mit der Neufassung hat das BKA außerdem das Recht erhalten, präventive Ermittlungen ohne konkreten Tatverdacht in eigener Regie durchzuführen. Abhörmaßnahmen dürfen auch gegen Berufsgeheimnisträger (§ 53 StPO) mit Ausnahme der Verteidiger, Abgeordneten und Geistlichen einer staatlich anerkannten Religionsgemeinschaft durchgeführt werden (§ 20 u BKA-Gesetz).

Am 27. Januar 2009 haben insbesondere mehrere Journalisten Verfassungsbeschwerde gegen das Gesetz eingereicht. Hierüber ist noch nicht entschieden.

### 3.2 Sicherheit in der Informationstechnik (BSI-Gesetz)

Um die aktuellen Bedrohungen zu bekämpfen und der zunehmenden Bedeutung der Informations- und Kommunikationstechnologie in der heutigen Gesellschaft Rechnung zu tragen, wurden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Novellierung des BSI-Gesetzes weitere Aufgaben und Befugnisse eingeräumt:

- Nach § 4 BSI-Gesetz wird das BSI als zentrale Meldestelle für IT-Sicherheit Informationen über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik sammeln und auswerten.
- Darüber hinaus erhält das BSI gem. § 5 BSI-Gesetz die Befugnis, Protokolldaten sowie Daten, die an den Schnittstellen der Kommunikationstechnik des Bundes anfallen, zu erheben, auszuwerten, zu speichern, zu verwenden und zu verarbeiten.
- Nach § 7 BSI-Gesetz darf das BSI Informationen und Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten sowie vor Schadprogrammen an die betroffenen Stellen oder die Öffentlichkeit weitergeben. Zunächst besteht dabei grundsätzlich die Pflicht, den Hersteller vorab zu informieren.
- Das BSI ist zudem befugt, einheitliche und strenge Sicherheitsstandards für die Bundesverwaltung zu definieren und bei Bedarf geeignete Produkte entwickeln zu lassen bzw. auszuschreiben und bereitzustellen (§ 8 BSI-Gesetz).

Nach Ansicht des Bundesdatenschutzbeauftragten gehen allerdings die vorgesehenen Befugnisse der beim Innenministerium angeschlossenen Behörde zu weit.

In der Tat geben die Regelungen dem BSI die Möglichkeit, »die gesamte Sprach- und Datenkommunikation aller Unternehmen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung abzuhören und auszuwerten«.

Problematisch ist es auch, dass das BSI nicht verpflichtet ist, ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Wirtschaft und Gesellschaft vor zu erwartenden Angriffen in Form etwa von Spionage oder Sabotage zu warnen.

Zu weit geht darüber hinaus aus Datenschutzsicht die Erlaubnis zur Datenübermittlung an den Verfassungsschutz sowie an Strafverfolgungsbehörden selbst bei nicht erheblichen, im Zusammenhang mit der Telekommunikation begangenen Delikten. Auch gegen dieses Gesetz wurde u. a. von einem Bundestagsabgeordneten der Grünen Verfassungsbeschwerde eingereicht. Hier wird geltend gemacht, dass die dem BSI erlaubte Kommunikations- und Surfprotokollierung direkt durch den Staat erfolgen und sogar die aufgerufenen Internetseiten umfassen darf. Dies mache die Regelung von Grund auf verfassungswidrig, wenn man die Maßstäbe des Verfassungsgerichtsurteils zur Vorratsdatenspeicherung zugrunde legt.

### 3.3 Drei neue BDSG-Novellen im Jahr 2009

Der Bundestag hat im Jahre 2009 das Bundesdatenschutzgesetz (BDSG) innerhalb weniger Monate dreimal geändert und dies in drei verschiedenen Gesetzen. Für den WDR sind diese Novellen allerdings von geringerer Bedeutung, da auf den WDR nicht das Landesdatenschutzgesetz, sondern das Landesdatenschutzgesetz Nordrhein-Westfalen Anwendung findet. Hier bleibt allerdings abzuwarten, inwieweit der Landesgesetzgeber Regelungen aus den BDSG-Novellierungen zukünftig in das Landesdatenschutzgesetz übernehmen will.

**BDSG-Novelle 1 – Inkrafttreten zum 1. April 2010**
Ziel der sog. BDSG-Novelle 1 ist es, die Tätigkeit von Auskunfteien und ihrer Vertragspartner (insbesondere Kreditinstituten) transparenter zu machen, indem Informations- und Auskunftsrechte von Betroffenen gestärkt werden sollen. Des Weiteren enthält das Gesetz spezifische Erlaubnistatbestände und Regelungen für Scoring-Verfahren. Dies sind mathematisch-statistische Verfahren zur Berechnung der Wahrscheinlichkeit eines bestimmten Verhaltens, insbesondere zur Kreditwürdigkeit einer Person. Der Gesetzgeber hat dazu zwei völlig neue Tatbestände (§ 28 a – Datenübermittlung an Auskunfteien und § 28 b – Scoring) geschaffen. Die Norm zur Auskunfterteilung an den Betroffenen (§ 34) wurde völlig überarbeitet und neu gefasst. Schließlich wurden § 6 a (Automatisierte Einzelfallentscheidung), § 35 (Berichtigung, Sperrung und Löschung) geändert und die Bußgeldtatbestände in § 43 Abs. 1 erweitert.

**BDSG-Novelle II – Inkrafttreten 1. September 2009:**
Diese umfangreichste Novelle hatte zunächst zum Ziel, nicht nur das BDSG grundlegend zu reformieren, sondern auch ein Auditierungsverfahren (Zertifizierungsverfahren) einzuführen. Im Laufe des Gesetzgebungsverfahrens ist indessen der Entwurf für ein Datenschutzauditgesetz fallen gelassen worden. Im BDSG selbst wurden jedoch 18 Paragrafen geändert. Dabei lassen sich mehrere große Bereiche darstellen:

- Änderungen des Listenprivilegs beim Adresshandel, Neuregelung für Markt- und Meinungsforschung, Opt-In-Koppelungsverbot; es gelten Übergangsregelungen für die Werbung bis 31. August 2012
- Beschäftigtendatenschutz (insbesondere Arbeitnehmer in der Privatwirtschaft)
- Auftragsdatenverarbeitung
- Neue Befugnisse für die Aufsichtsbehörden und neue oder stark erweiterte Bußgeldtatbestände
- Informationspflichten bei Datenschutzverstößen
- Besonderer Kündigungsschutz für Datenschutzbeauftragte; Änderungen im Telekommunikationsgesetz und Telemediengesetz

**BDSG-Novelle III – Inkrafttreten am 11. Juni 2010**
Im Rahmen des Gesetzes zur Umsetzung der EU-Verbraucherkreditrichtlinie sind nicht nur umfangreiche Änderungen im BGB (z. B. zum Darlehnsvertrag) erfolgt, sondern auch § 29 BDSG wurde um zwei Absätze erweitert und mit einer Bußgeldbewertung versehen. Diese Erweiterung schafft Pflichten für Datenbankbetreiber, deren sich Darlehnsgeber zur Bewertung der Kreditwürdigkeit potenzieller Darlehnsnehmer bedienen.

### 3.4 Arbeitsmedizinische Vorsorgeuntersuchungen

Aufgrund der §§ 18 und 19 des Arbeitsschutzgesetzes (ArbSchG) wurde die »Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) vom 18. Dezember 2008« (BGBl. I Seite 2768) erlassen. Sie enthält Regelungen zu den arbeitsmedizinischen Vorsorgeuntersuchungen. Diese umfassen sog. Pflichtuntersuchungen, Angebotsuntersuchungen und Wunschuntersuchungen (§ 2 Abs. 3 ArbMedVV), für die vorrangig der nach § 2 Arbeitssicherheitsgesetz bestellte Betriebsarzt beauftragt werden soll:

– Pflichtuntersuchen (§ 4 ArbMedVV) müssen vom Arbeitgeber angeboten werden, und er hat Sorge dafür zu tragen, diese als Erstuntersuchung und dann als regelmäßige Nachuntersuchungen durchzuführen. Für Pflichtuntersuchungen hat der Arbeitgeber eine Vorsorgekartei mit Angaben über Anlass, Tag und Ergebnis seiner Untersuchung zu führen (die Kartei kann auch automatisiert geführt werden). Die Angaben sind bis zur Beendigung des Beschäftigungsverhältnisses aufzubewahren, dem Betroffenen ist mit Beendigung eine Kopie auszuhändigen und die Daten sind anschließend zu löschen. Für Pflichtuntersuchungen hat der Arzt den Untersuchungsbefund und das Untersuchungsergebnis schriftlich festzuhalten, die untersuchte Person darüber zu beraten und ihr eine Bescheinigung auszustellen. Diese Bescheinigung enthält Angaben über den Untersuchungsanlass und den Tag der Untersuchung sowie die ärztliche Beurteilung, ob und inwieweit bei der Ausübung einer bestimmten Tätigkeit gesundheitliche Bedenken bestehen. Nur im Falle dieser Pflichtuntersuchung enthält der Arbeitgeber eine Kopie der Bescheinigung.

– Angebotsuntersuchungen (§ 5 ArbMedVV) müssen nur angeboten werden (ebenfalls regelmäßig), und zwar auch dann immer, wenn ein Arbeitnehmer einmal ein Angebot ausschlägt. Für Angebotsuntersuchungen (z. B. für Bildschirmarbeitsplätze) sieht der Gesetzgeber weder eine Bescheinigung noch die Weitergabe der Bescheinigung in Kopie an den Arbeitgeber vor. Der Betriebsarzt könnte aber mit Einwilligung des Betroffenen eine Bescheinigung ausstellen, damit der Betroffene sie dann nach seiner freien Entscheidung an den Arbeitgeber weitergibt oder nicht. Eine arbeitgeberseitig vorformulierte Einwilligung bzw. ein vom Arbeitgeber gestelltes Formular oder gar die Aufforderung des Arbeitgebers, dem Vorgesetzten (wenn auch nur beschränkte) Untersuchungsergebnisse über die arbeitsmedizinische Vorsorgeuntersuchung weiterzugeben, dürfte deshalb grundsätzlich nicht zulässig sein.

Im Geltungsbereich des Landesdatenschutzgesetzes NRW, und somit auch beim WDR, sieht allerdings § 29 Abs. 3 DSG NRW vor, dass zum Zwecke der Eingehung eines Dienst- oder Arbeitsverhältnisses ärztliche oder psychologische Untersuchungen und Tests durchgeführt werden dürfen. Die Weiterverarbeitung ist aber nur mit schriftlicher Einwilligung der betroffenen Person zulässig. Die Einstellungsbehörde – also auch der WDR – darf vom untersuchenden Arzt – in der Regel dem Betriebsarzt – grundsätzlich nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und dabei festgestellter Risikofaktoren verlangen.

Diese Verfahrensweise wurde im WDR nochmals in Absprache zwischen der HA Personal, dem Betriebsarzt und dem Datenschutzbeauftragten abgestimmt.

### 3.5 Volkszählung 2011 (Zensusgesetz)

Fast genau 24 Jahre nach der letzten Volkszählung gibt es in Deutschland gegenwärtig wieder ein solche, und zwar zum Stichtag 9. Mai 2011. Die Durchführung in Deutschland wird im Zensusgesetz 2011 vom 8. Juli 2009 (BGBl. Seite 1781) geregelt und ist Folge der EU-Verordnung 763/2008 vom 9. Juli 2008, in welcher auch die zu erhebenden Daten festgelegt worden sind. In Deutschland wird keine traditionelle, sondern eine registergestützte Volkszählung durchgeführt, denn die Daten stammen überwiegend aus Registern, insbesondere dem Melderegister und dem Register der Bundesanstalt für Arbeit. Informationen über die Gebäude und Wohnungen, die nicht flächendeckend durch die Verwaltung erfasst sind, werden daneben per Post bei den Gebäude- und Wohnungseigentümern erhoben. Andere Fragen, wie etwa zur Bildung und Ausbildung oder über die Erwerbstätigkeit, werden nur bei einem kleinen Teil der Einwohnerinnen und Einwohner in Form repräsentativer Stichproben erhoben. Weitere Informationen sind über die Adresse www.zensus2011.de erhältlich.

### 3.6 ELENA – der elektronische Entgeltnachweis

ELENA ist die Abkürzung für »elektronischer Entgeltnachweis«. Ziel dieses früher unter dem Begriff Job-Card geplanten Verfahrens ist es, bisher vom Arbeitgeber per Papier erstellte (Gehalts-)Bescheinigungen, welche für Sozialleistungen benötigt werden, zu ersetzen. In der ELENA-Datenbank werden ab 1. Januar 2010 alle Daten gespeichert, die bislang in Antragsverfahren vor Sozialbehörden (Arbeitsagentur, Wohngeldstelle, Elterngeldstelle) auf amtlichen Vordrucken erhoben wurden. Es handelt sich dabei nicht nur um Einkommensdaten, sondern auch um weitere Anga-

ben, die für die Prüfung notwendig sind, ob ein Anspruch auf die Sozialleistung besteht oder nicht. Durch das Gesetz vom 28. März 2009 (BGBl. Seite 634) sind alle Arbeitgeber gesetzlich verpflichtet, monatlich eine entsprechende ELENA-Meldung an eine bundesweite zentrale Speicherstelle zu versenden, damit die bisher vom Arbeitgeber auf Papier erstellten Gehaltsbescheinigungen in Verfahren vor Sozialbehörden elektronisch zur Verfügung stehen. Erfasst werden aber nicht nur Arbeitnehmer, sondern alle Beschäftigten. Datenschutzproblematisch ist zum einen die damit verbundene zeitlich unbefristete Vorratsdatenspeicherung, zumal auch Daten von Personen gespeichert werden, die wahrscheinlich nie eine entsprechende soziale Leistung beantragen werden. Aber auch der Umfang und die Sensibilität der zwangsweise zu übermittelnden Daten sind problematisch. Denn Monat für Monat sollen 3 Mio. Arbeitgeber die Einkommensdaten von über 30 Mio. Beschäftigten übermitteln, und zwar für eine zeitlich unbegrenzte Speicherung. Auch der WDR ist verpflichtet, die entsprechenden Meldungen durchzuführen, und kommt dieser Verpflichtung – wenn auch nicht frei von Bedenken – nach. Auch hier haben inzwischen mehrere Tausend Personen Verfassungsbeschwerde gegen das ELENA-Gesetz eingelegt.

### 3.7 Landesgesetzgebung – Rundfunkrechtliche Staatsverträge

Die maßgeblichen Regelungen für die Rundfunkanstalten finden sich im Rundfunkstaatsvertrag (RfStV), dem Rundfunkgebührenstaatsvertrag (RGebStV) sowie dem Rundfunkfinanzierungsstaatsvertrag. Wenn das entsprechende Ratifizierungsverfahren in allen Bundesländern erfolgreich abgeschlossen worden ist, tritt zum 1. Januar 2013 an die Stelle des Rundfunkgebührenstaatsvertrages der neue Rundfunkbeitragsstaatsvertrag als Teil des 15. Rundfunkänderungsstaatsvertrages.

Mit dem seit 1. September 2008 geltenden 10. Rundfunkänderungsstaatsvertrag wurden auch zwei datenschutzrechtliche Vorschriften präzisiert. So wurde zum einen der § 6 Abs. 2 RGebStV aufgenommen, der bestimmt, dass für eine Befreiung von der Gebührenpflicht nicht nur die Vorlage des im Gebührenstaatsvertrag genannten (Original-)Bescheides des Sozialleistungsträgers ausreichend ist, sondern auch eine entsprechende Bestätigung des jeweiligen Leistungsträgers. Damit wurde die Praxis der GEZ in Gesetzesform gegossen, denn schon bislang wurde z. B. die Bestätigung einer Behörde akzeptiert, wonach ein Antragsteller beispielsweise Arbeitslosengeld II für einen bestimmten Zeitraum erhält. Damit muss der Antragsteller nicht mehr den gesamten Bescheid mit zum Teil weiteren Daten bei der GEZ einreichen, sondern nur eine Bestätigung der Behörde als sog. Drittbescheinigung. Dieses datenschutzfreundliche Verfahren konnte allerdings erst eingeführt werden, nachdem gewährleistet war, dass seitens der entsprechenden Behörde die Daten verbindlich bestätigt werden.

Auch die zweite Änderung bewirkt eine datenschutzrechtliche Präzisierung und Klarstellung. Nachdem zunächst die Praxis der GEZ, von Adresshändlern bestimmte Anschriften zu erwerben, im Streit stand, hatte der Gesetzgeber mit dem 8. Rundfunkänderungsstaatsvertrag eine Klarstellung in § 8 Abs. 4 Rundfunkgebührenstaatsvertrag vorgenommen und damit für diese Praxis eine spezielle Rechtsgrundlage geschaffen. In der Folgezeit ging aber insbesondere die politisch motivierte Diskussion über die Zulässigkeit der sog. Mailings weiter. Der Gesetzgeber hat dann den weiten § 8 Abs. 4 mit einem pauschalen Verweis auf § 28 BDSG dahingehend geändert, dass jetzt ausdrücklich in § 8 Abs. 4 eine eigenständige Regelung getroffen wurde. Der pauschale Verweis auf § 28 ist damit entfallen. Die neue Vorschrift ist darüber hinaus wesentlich präziser und transparenter gestaltet. An der Neuformulierung waren sowohl die zuständigen Landesdatenschutzbeauftragten als auch die Rundfunkdatenschutzbeauftragten intensiv beteiligt.

### 3.8 Weitere Gesetzesvorhaben und Entwicklungen

Von herausragender Bedeutung auf Landesebene ist für die öffentlich-rechtlichen Rundfunkanstalten der 15. Rundfunkänderungsstaatsvertrag, mit dem nach erfolgter Ratifizierung durch die Länderparlamente der Wechsel von geräteabhängigen Rundfunkgebühren zu einem geräteunabhängigen Haushalts- und Betriebsstättenbeitrag vollzogen werden soll.

Die dort getroffenen Regelungen, an denen im Vorfeld auch die Landesdatenschutzbeauftragten wie auch die Rundfunkdatenschutzbeauftragten beteiligt waren, tragen im Ergebnis datenschutzrechtlichen Erwägungen ausreichend Rechnung.

Dabei soll nicht verhehlt werden, dass der von den Ministerpräsidentinnen und Ministerpräsidenten unterzeichnete Staatsvertrag nicht die datenschutzfreundlichsten Regelungen beinhaltet.

Insoweit ist zunächst verfahrensmäßig zu bemängeln, dass zwar ein Austausch zwischen den Landesdatenschutzbeauftragten und den Rundfunkdatenschutzbeauftragten im Rahmen des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder stattgefunden hat. Eine weitergehende Zusammenarbeit, die im Ergebnis zu einer gemeinsamen datenschutzrechtlichen Bewertung durch die Landesbeauftragten für den Datenschutz, soweit dort eine entsprechende Zuständigkeit gegeben ist, und den Rundfunkdatenschutzbeauftragten geführt hätte, wird allerdings von den Landesdatenschutzbeauftragten verweigert. Grund hierfür ist, dass die Landesdatenschutzbeauftragten mehrheitlich der Meinung sind, bei den Rundfunkdatenschutzbeauftragten handele es sich nicht um unabhängige Kontrollstellen im Sinne der EU-Datenschutzrichtlinie. Hierbei wird allerdings verkannt, dass z. B. die Regelung in § 53 Abs. 1 des WDR-Gesetzes eindeutig festlegt, dass der Rundfunkdatenschutzbeauftragte

des WDR vollumfänglich an die Stelle des Landesbeauftragten für den Datenschutz tritt, soweit es um die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften bei der gesamten Tätigkeit des WDR geht. Dies bedeutet, dass sich auch die Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten innerhalb seines Zuständigkeitsbereiches an den Regelungen für den Landesdatenschutzbeauftragten in § 22 des Datenschutzgesetzes NRW zu orientieren haben. Demzufolge gilt für den Datenschutzbeauftragten des WDR auch die Regelung in § 21 Abs. 6 Datenschutzgesetz NRW, dass er mit den Behörden und sonstigen Stellen zusammenarbeitet, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in der Europäischen Union, im Bund und in den Ländern zuständig sind. Hätte es hier eine intensivere Zusammenarbeit gegeben, hätten zum einen vermehrt datenschutzrechtliche Fragestellungen und Anregungen vonseiten der Landesdatenschutzbeauftragten auch durch die Rundfunkdatenschutzbeauftragten vertieft aufgegriffen werden können. Zum anderen wäre es aber auch möglich gewesen, seitens der Rundfunkdatenschutzbeauftragten die Sachnähe zur zu regelnden Materie einzubringen mit der Folge, dass im Rahmen der datenschutzrechtlichen Bewertung sachfremde und dem tatsächlichen Verfahrensablauf nicht entsprechende Darstellungen vermieden worden wären.

Inhaltlich ist es so, dass durch die Neuregelungen im 15. Rundfunkänderungsstaatsvertrag die bisherigen Nachforschungen bei den Bürgerinnen und Bürgern durch den Wegfall des Gerätebezugs auf ein Minimum reduziert werden können. Fragen nach dem Vorhandensein von Rundfunkempfangsgeräten entfallen. Auch der datenschutzrechtliche Grundsatz der Direkterhebung, wonach Daten grundsätzlich beim Betroffenen erhoben werden sollen, bleibt gewahrt. Die außerdem vorgesehene Möglichkeit der Datenerhebung bei Dritten ohne Kenntnis des Betroffenen ist eindeutig als Uultima Ratio formuliert.

Andererseits umfassen die vom Beitragspflichtigen gegenüber den Landesrundfunkanstalten mitzuteilenden Daten zukünftig nicht nur die Anschrift der Wohnung, sondern »alle vorhandenen Angaben zur Lage der Wohnung«.

Hier ist aus datenschutzrechtlicher Sicht sicherlich ernsthaft zu fragen, welche Daten im Ergebnis sensibler sind. Die Angabe, dass ein Herr X in der Y-Straße 233 ein Hörfunk- oder ein Fernsehgerät zum Empfang bereithält, ist nach meiner Bewertung im Ergebnis weniger sensibel als die Tatsache, dass nunmehr mitzuteilen ist, dass der Herr X in der Y-Straße 233 in der dritten Wohnung links in der vierten Etage wohnt.

Dem teilweise vorhandenen weitergehenden Wunsch, zu einer Wohnung auch sämtliche volljährigen Wohnungsinhaber zu erfassen und zu speichern, hat der Gesetzgeber allerdings auch unter Berücksichtigung entsprechender Stellungnahmen seitens der Datenschutzbeauftragten einen Riegel vorgeschoben.

Auch ein weiteres Problem ist in diesem Zusammenhang anzusprechen:

Nach § 14 Abs. 9 des Rundfunkbeitragsstaatsvertrages findet bezogen auf einen Stichtag ein einmaliger Meldedatenabgleich mit den Meldebehörden zum Zwecke der Bestands- und Ersterfassung von Beitragsschuldner statt.

Im Hinblick auf die Umstellung von der gerätebezogenen Rundfunkgebühr auf den wohnungsbezogenen Rundfunkbeitrag ist diese einmalige Übermittlung im Grundsatz datenschutzrechtlich nicht zu beanstanden. Problematisch ist allerdings, dass der Gesetzgeber in § 14 Abs. 8 des Rundfunkbeitragsstaatsvertrages unter Ziffer 7 in durchaus sinnvoller Weise festgelegt hat, dass die gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnung, einschließlich aller vorhandenen Angaben zur Lage der Wohnung, zu übermitteln sind. Für die Umsetzung des Rundfunkbeitragsstaatsvertrages ist es auch erforderlich, dass Beitragsschuldner nicht nur einer bestimmten Adresse, sondern einer konkreten Wohnung zugeordnet werden können. Letztlich ist Voraussetzung für das Funktionieren der Erhebung des Rundfunkbeitrages eine funktionsfähige Wohnungsdatenbank. Tatsache ist aber, dass die Mehrzahl der Einwohnermeldeämter nicht über Angaben zur Lage der Wohnung verfügen und diese Daten somit nicht übermitteln können. Aus diesem Grunde ist vorgesehen, dass die GEZ eine eigene Objektdatenbank erstellt, wobei leider bislang die hierfür erforderlichen Details den Datenschutzbeauftragten nicht mitgeteilt worden sind. Hier bestehen nach wie vor Zweifel, dass tatsächlich in allen Fällen eine korrekte Zuordnung der bisherigen Rundfunkteilnehmer zu einer konkreten Wohnung erfolgen kann und ebenso die Zuordnung neuer Beitragsschuldner zu einer korrekten Wohnung. Hier besteht die Gefahr, dass Beitragsschuldner zum einen nicht erfasst werden und zum anderen eine Mehrfacherfassung erfolgt.

# C Datenschutz im WDR

## 1. Online-Aktivitäten

### 1.1 Datenschutzrichtlinie für soziale Netzwerke im Rundfunkbereich

Interaktiver Austausch im Internet ist etwas, auf das immer weniger Menschen verzichten wollen. Sog. soziale Netzwerke bieten eine Plattform, die virtuelle Begegnung am Computer. Namen wie *Facebook*, *Wer-kennt-wen*, *StudiVZ*, *Myspace* und andere bilden die Treffpunkte und Stammtische der digitalen Welt mit zunehmender Popularität. Unter dem Schlagwort Web 2.0 tummeln sich diese sozialen Netzwerke, Blogs (eine Art öffentliches Tagebuch), Foren, Tauschbörsen und Videoportale und bieten einen weltweiten Austausch von Meinungen und teilweise auch sehr subjektiv gefärbten Informationen.

Auch der Bereich des Rundfunks hat diese Form der Kommunikation mit seinen Nutzern bereits in mehreren Programmen umgesetzt. Auch in Communities des WDR tauschen sich Nutzer untereinander aus, und dies überwiegend unter der Leitung und Überwachung der jeweiligen Redaktionen. Die Teilnehmer können eigene Videos, Bilder, Musik usw. einstellen, ihre Meinungen austauschen, Kontakte knüpfen und Interessengruppen bilden. Diese Form eines »erweiterten Rundfunkangebotes« (rechtlich dürfte es sich hier um Telemedien handeln) verstärkt die Bindungen und ermöglicht auch die Rückkopplung zu den WDR-Programmen.

Datenschutzrechtlich kritisch ist allerdings die Sorglosigkeit und Naivität der Nutzer dieser Plattformen im Umgang mit ihren persönlichen Daten. Wenn zu viele persönliche Daten preisgegeben werden, bietet das den verschiedensten Sammlern und Nutzern solcher Daten, die keineswegs immer legitime Zwecke verfolgen, ein wahres Schlaraffenland. Das oberste Gebot lautet deshalb, dass das Netz nichts vergisst. Auch wenn man nichts zu verbergen hat, so das häufig genutzte Argument der Nutzer, kann doch das Offenlegen der Privatsphäre am Ende verhängnisvoll sein und zu Datenmissbrauch führen. Sparsamkeit in der Datenpreisgabe und höchstmögliche Anonymität sind der beste Schutz.

Aufgrund der drängenden Problematik im Zusammenhang mit sozialen Netzwerken im Bereich des Rundfunks hat der Arbeitskreis der Rundfunkdatenschutzbeauftragten Richtlinien für eine datenschutzkonforme Gestaltung sozialer Netzwerke erarbeitet, die den einzelnen Redaktionen zur Unterstützung und als Leitfaden für ihre Online-Angebote dienen sollen. Dieser Leitfaden, der auch im WDR publiziert ist, ist als Orientierung gedacht und ersetzt nicht die Beratung der Redaktionen durch den Datenschutzbeauftragten persönlich, die auch in großem Umfang wahrgenommen wird. Von den einzelnen empfohlenen Datenschutzmaßnahmen des Leitfadens »Datenschutz und Datensicherheit in sozialen Netzwerken im Web 2.0 der Rundfunkanstalten« seien als wichtigste Punkte kurz angeführt:

- Beschränkung der Pflichtangabe der Netzwerkteilnehmer auf das notwendige Minimum
- Unterrichtung der Nutzer über Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten, über die Möglichkeit des Widerrufs der pseudonymen Nutzung sowie der Verwendung von Cookies in Form einer Datenschutzerklärung
- Differenziertes Berechtigungskonzept, das dem Nutzer ermöglicht festzulegen, welche Informationen für andere Nutzer der Communities sichtbar sein sollen
- Der Zugriff auf sensible personenbezogene Daten der Nutzer durch Nichtmitglieder des Netzwerkes von außen (z. B. bei Suchmaschinen) muss technisch ausgeschlossen sein
- Technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten vor Missbrauch, Verlust und Verfälschung müssen ein hohes Datenschutzniveau gewährleisten

### 1.2 Jugendliche und Datenschutz

Persönliche Daten von Jugendlichen (Minderjährigen), die innerhalb des WDR insbesondere vom Programm 1LIVE angesprochen werden, unterliegen einem besonderen Schutz. Auch insoweit hat beim WDR die Sicherheit der Jugendlichen, die sich etwa bei 1LIVE tummeln, höchste Priorität. Auch hier wurde ich mehrmals zu Beratungsgesprächen hinzugezogen und konnte mich vergewissern, dass den datenschutzrechtlichen Bestimmungen hohe Priorität eingeräumt wird.

Dass die Arbeit der Redaktion insoweit sehr effektiv ist, zeigt sich u. a. auch daran, dass es keinen Fall gegeben hat, in dem sich etwa besorgte Eltern im Hinblick auf die Erhebung personenbezogener Daten ihrer Kinder an mich gewandt haben.

Richtig ist allerdings, dass ein Mindestmaß an personenbezogenen Daten erhoben werden muss, um sich im Falle einer missbräuchlichen Nutzung an die Erziehungsberechtigten, in der Regel die Eltern, wenden zu können.

### 1.3 Datenumfang bei der Nutzung von Online-Angeboten

Mit der zunehmenden Berichterstattung in den Medien über missbräuchliche Nutzung von Daten steigt auch die Sensibilisierung der Rundfunkteilnehmer für ihre persönlichen Daten, die sie etwa im Rahmen von Online-Angeboten an die einzelnen Programmredaktionen des WDR übermitteln. Tatsache ist aber auch hier, dass in allen Fällen

eine datenschutzkonforme Behandlung der Nutzerdaten von WDR-Online-Angeboten erfolgt. Auch dies zeigt sich daran, dass es im Wesentlichen keine datenschutzrechtlichen Beschwerden in diesem Punkt gegeben hat.

Gleichwohl gibt es einen Punkt, der noch einer abschließenden datenschutzrechtlichen Klärung bedarf.

Ein Nutzer des Online-Angebotes des WDR hat sich nachhaltig darüber beschwert, dass seine personenbezogenen Daten wie IP-Adresse beim WDR 90 Tage lang gespeichert werden.

Die Behandlung dieser Beschwerde ist noch nicht abgeschlossen.

Grundsätzlich ist bei der Verarbeitung personenbezogener Daten durch den WDR das Landesdatenschutzgesetz NRW anwendbar, das keinerlei Speicherfristen vorsieht. Es heißt dort lediglich in § 13 Abs. 1, dass die Speicherung zulässig ist, wenn es zur rechtmäßigen Erfüllung der Aufgaben zulässig ist. Nach § 19 Abs. 3 sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

WDR-intern ist geregelt, dass die Speicherung und Verarbeitung von Benutzerinformationen u. a. auf die Gewährleistung der Systemsicherheit und die Behebung von Fehlern und auf Wartungs- und Supportzwecke begrenzt ist. Der Zugriff auf die entsprechenden Systemfunktionen ist nur den für den Betrieb der Datenverarbeitungssysteme zuständigen Bereichen sowie der Revision vorbehalten.

In einer weiteren internen Dienstvereinbarung heißt es, dass sämtliche im Rahmen der Systemprotokollierung gespeicherten Daten spätestens nach 90 Tagen gelöscht werden. Dies bedeutet zum einen allerdings nicht, dass die Daten zwingend 90 Tage aufzubewahren sind. Vielmehr ist der Zeitraum als maximale Obergrenze zu sehen. Darüber hinaus ist zu berücksichtigen, dass es sich hier um eine Regelung für den Dienstbetrieb innerhalb des WDR handelt. Folglich ist Gegenstand dieser Regelung nur die Protokollierung von Daten von WDR-Mitarbeiterinnen und -Mitarbeitern. Das Übertragen dieser Regelung auf die Protokollierung von personenbezogenen Daten externer Nutzer ist zunächst jedenfalls nicht nachvollziehbar.

Gegenwärtig wird auch überlegt, den Zeitraum deutlich zu verkürzen, weil sich herausgestellt hat, dass bei der Auswertung und Behebung von Störungen und bei Missbrauchsverdacht ein kürzerer Zeitraum, der noch exakt zu definieren ist, ausreichend sein dürfte. Soweit es um die in der Beschwerde angesprochene IP-Adresse geht, ist zu sagen, dass nach der höchstrichterlichen Rechtsprechung des Bundesgerichtshofes (Urteil vom 12. Mai 2010 – I ZR 121/08) der IP-Adresse keine Identifikationsfunktion zukommt. Sie ist keinem konkreten Nutzer zugeordnet, sondern nur einem Anschluss, bei dem grundsätzlich die Möglichkeit besteht, dass jede beliebige Person diesen Anschluss nutzen kann. Die IP-Adresse gibt deshalb bestimmungsgemäß keine zuverlässige Auskunft über die Person, die zu einem konkreten Zeitpunkt den Anschluss genutzt hat, ja nicht einmal über den Anschlussinhaber selbst. Erst wenn etwa über den Provider aufgrund der IP-Adresse der konkrete Anschlussinhaber in Erfahrung gebracht wird, was nur mit gerichtlicher Hilfe geht, wird aus der IP-Adresse ein personenbezogenes Datum. Eine solche Zuordnung ist jedoch im Regelfall nur innerhalb von sieben Tagen möglich, da die Verbindungsdaten danach vom Provider zu löschen sind (BGH-Urteil vom 13. Januar 2011 – III ZR 146/10). Im Ergebnis ist es deshalb so, dass auch der WDR, selbst wenn die IP-Adresse noch vorgehalten werden sollte, nach sieben Tagen im Regelfall keine Auskunft über den Anschlussinhaber mehr erlangen kann.

Gleichwohl sollte aus datenschutzrechtlicher Sicht wie ausgeführt die Höchstdauer der Speicherung personenbezogener Daten von Nutzern überdacht und deutlich verkürzt werden.

### 1.4 Gewinnspiele und der Umgang mit Adressen der Hörer/-innen und Zuschauer/-innen

Schlagzeilen über missbräuchliche Nutzung personenbezogener Daten haben sich, worauf ich auch an anderer Stelle hingewiesen habe, in den letzten Jahren gehäuft. Immer mehr machen sich Zweifel breit, ob die eigenen Daten wirklich in guten Händen sind. Vor allem auch der nach EU-Normen erlaubte florierende Handel mit Adressen gerät zunehmend ins Kreuzfeuer der Kritik. Vor diesem Hintergrund besitzt der korrekte Umgang mit den Adressen der Hörer und Zuschauer, die im Rahmen von Gewinnspielen, Umfragen, Zeitschriftenabonnements (etwa WDR-Print), Newslettern und Programmaktionen im WDR gewonnen werden, höchste Priorität.

Von den privaten Rundfunk- und Fernsehanstalten ist bekannt, dass sie die legitime Möglichkeit nutzen, mit dem Verkauf von Adressen ihrer Hörer und Zuschauer ihr Budget zu erweitern. Vor allem der Rücklauf von Programmaktionen, aber auch unaufgeforderte Zuschriften und Anfragen ermöglichen den Aufbau großer Adressdateien, die Auswertungen zulassen und so zum gewinnbringenden Handelsobjekt werden. Auch Zeitschriftenverlage, der Versand- und Internethandel sowie Firmen mit lockenden Preisausschreiben liefern Datenmaterial zum Aufbau von qualifizierten Datenbeständen für den gewerblichen Adresshandel.

Im Gegensatz zu den privaten Gesellschaften gelten für die öffentlich-rechtlichen Rundfunkanstalten die strengen datenschutzrechtlichen Bestimmungen für Behörden und öffentliche Stellen. Für den WDR bedeutet das konkret, dass die Adressen aus Zuschriften von Hörern und Zuschauern nicht weitergegeben werden dürfen. Im Fall der Verwendung für eigene Zwecke im Rahmen von Programmaktionen muss die ausdrückliche Zustimmung der Adressaten vorliegen. Nicht zuletzt um sich von der Praxis der privaten Rundfunkveranstalter abzugrenzen, ist es besonders wichtig, dass der öffentlich-rechtliche Rundfunk vorbildlich, unter Beachtung aller datenschutzrechtlichen Vorgaben, dem

Vertrauen seiner Hörer und Zuschauer begegnet. Auch aus den Redaktionen des WDR erreichen mich gelegentlich Anfragen, wie im Falle von Gewinnspielen und anderen Programmaktionen mit den Adressdaten zu verfahren ist.

Auf die wichtigsten Punkte möchte ich hier nochmals hinweisen:

- In den Teilnahmebedingungen muss ein Datenschutzhinweis enthalten sein, der auf die restriktive Verwendung der Adresse abstellt und die Weitergabe der Adressdaten an Dritte ausschließt. Wird im Wege der Auftragsverarbeitung ein Dritter mit der Durchführung der Aktion beauftragt, ist sicherzustellen, dass er sich den entsprechenden für den WDR geltenden Regularien unterwirft und eine entsprechende Sicherheitsvereinbarung abgeschlossen wird.
- Die Teilnehmer müssen in die Teilnahmebedingungen unter Verwendung ihrer Adresse ausdrücklich einwilligen. Üblicherweise kann die Teilnahme durch Setzen eines Häkchens in einem dafür vorgesehenen Feld oder durch Drücken eines Buttons im Falle von Online-Aktionen erwirkt werden.
- Für die Verwendung der Adresse zu einem späteren Zeitpunkt im Rahmen weiterer Programmaktionen (Eigenwerbung) muss der Teilnehmer vorab informiert werden und ebenfalls ausdrücklich einwilligen.
- Eine einmal erteilte Einwilligung kann der Adressat jederzeit widerrufen. Als Folge ist die Adresse aus dem Datenbestand zu löschen. Auch über die Möglichkeit ist der Teilnehmer zu informieren.
- Auf den Umstand, dass im Falle eines Gewinns oder im Verlauf einer Programmaktion der Name veröffentlicht werden kann, ist ebenfalls hinzuweisen.

## 2. Datenschutz in den SAP-gesteuerten Modulen (FI, CO, COGHOS, MM usw.)

Hier wird gegenwärtig ein Berechtigungsrahmengesetz erstellt, das Festlegungen zu Datenschutz-relevanten Themenstellungen im Rahmen der Einführung und des Betriebs von SAP-R/3-Systemen und Applikationen beim Westdeutschen Rundfunk enthält.

Das Berechtigungsrahmenkonzept hat die Aufgabe, die allgemeinen Rahmenbedingungen auf Basis der gesetzgeberischen und unternehmerischen Anforderungen an den Datenschutz und die Datensicherheit sowie Maßnahmen zu deren Einhaltung zu definieren.

Ziel des Berechtigungskonzeptes ist es, die WDR-SAP-Systeme vor Risiken zu schützen und die Datenintegrität sicherzustellen. Das Berechtigungskonzept behandelt die notwendigen Festlegungen für die Anwendungs- und Präsentationsebene im SAP R/3. Nicht eingeschlossen sind Sicherheitsfragen auf Betriebssystem-, Datenbank- und Kommunikationsebene.

Hierfür liegen eigene Konzepte vor bzw. müssen noch erarbeitet werden. Der Geltungsbereich des bereits vorliegenden Konzeptes erstreckt sich beim WDR auf die Berechtigungen innerhalb der vorhandenen SAP-R/3-System-Landschaft. Das Berechtigungsrahmenkonzept beschreibt die technischen und organisatorischen Zugriffsberechtigungsverfahren, die grundlegenden technischen Festlegungen, die Prozesse zur Erstellung von Berechtigungen sowie den Nachweis der sachgerechten Vergabe von Berechtigungen für das Entwicklungs-, Konsolidierungs- und das Produktivsystem.

Es stellt ferner eine Verfahrensanweisung für die Entwicklung der fachlichen Berechtigungskonzepte in den beteiligten Koordinationsbereichen dar und beschreibt so die Vorgehensweise, wie die Tätigkeiten in den Koordinationsbereichen von der Konzeption bis zur Freigabe von Berechtigungen optimal unterstützt werden können, ohne die bestehenden gesetzlichen und internen Anforderungen zu verletzen. Adressaten des Konzeptes sind all diejenigen WDR-Mitarbeiter/-innen, die im Rahmen von SAP-Einführungsprojekten Berechtigungen und Rollen konzipieren müssen und im produktiven Betrieb Rollen, Berechtigungen und SAP-Anwender administrieren bzw. das Konzept und die Verfahren prüfen und überwachen sollen.

### 2.1 Ziel des WDR-Berechtigungskonzepts

Mit der Einführung eines SAP-R/3-Berechtigungskonzepts beim Westdeutschen Rundfunk soll grundsätzlich die sichere, ordnungsgemäße und wirtschaftliche Bereitstellung von Daten

- für Abrechnungszwecke entsprechend den gesetzlichen Auflagen
- für Informationszwecke zur Unternehmenssteuerung gewährleistet werden.

An das SAP-R/3-Berechtigungskonzept werden hierbei folgende Anforderungen gestellt:

- Sicherstellung der Richtigkeit, Vollständigkeit und zeitgerechten Verfügbarkeit der Daten
- Gewährleistung der Nachvollziehbarkeit und Prüfbarkeit der Daten sowie des zweckgebundenen Gebrauchs
- Schutz vor Manipulation, Sabotage, Löschung und unberechtigter Einsichtnahme von Daten
- Schutz von personenbezogenen Daten und sensiblen Unternehmensdaten
- Transparenz in den Verfahren zur Anlage und Vergabe von Berechtigungen Zielsetzung
- Berechtigungsrahmenkonzept SAP R/3 Enterprise 9. Februar 2004
- Sichern von immateriellen Vermögenswerten

Hierdurch soll u. a. sichergestellt werden, dass keine unautorisierten, unvollständigen, unrichtigen und zeitlich oder sachlich falsch zugeordneten Daten in das System gelangen.

### 2.2 Sicherstellung der Revisionsfähigkeit des WDR-Berechtigungskonzepts

Das Rahmenkonzept wird sowohl der internen Revision beim WDR als auch dem externen Jahresabschlussprüfer zur Prüfung und Abstimmung vorgelegt. Die Personalvertretung (Personalrat) und der Datenschutzbeauftragte werden über die Erarbeitung des WDR-Berechtigungskonzepts informiert.

Im Rahmen dieses Konzeptes werden datenschutzrechtliche Erfordernisse beachtet.

## 3. Absicherung von Produktionsgewerken vor Bedrohungen aus dem Internet

### 3.1 Besondere Gefährdung der Produktions-IT

Die Produktions-IT ist aus Sicht der IT-Sicherheit besonders verwundbar und damit besonders stark durch Bedrohungen aus dem Internet gefährdet und unterliegt daher besonderen Anforderungen. Die Geräte sind produktionsrelevant, oft sogar senderelevant. Das bedeutet, dass ein Ausfall dieser Geräte Produktions- oder Sendestörungen zur Folge haben kann. Gleichzeitig sind die Installationen relativ statisch, d. h., die eingesetzten Betriebssysteme wie auch die eingesetzte Software können häufig nicht mit den Updatefrequenzen aktualisiert werden, die in der IT geboten sind. Verstärkend kommt hinzu, dass diese Geräte oft individuell konfiguriert sind und meist keine Anbindung an eine Softwareverteilung haben, sodass sie aufwendig händisch aktualisiert werden müssen. Daher sind diese Geräte besonders anfällig gegen Bedrohungen, insbesondere aus dem Internet.

### 3.2 Schutzsoftware nur beschränkt wirksam

Bedrohungen aus dem Internet können von Sicherheitssoftware nicht immer erkannt werden, das gilt verstärkt, wenn Betriebssysteme und Sicherheitssoftware nicht tagesaktuell gehalten werden.

Hier werden beispielhaft zwei Fälle erläutert:

**Java**
Die Version 1.6.19 kann jeden beliebigen Code auf einem System ausführen, sobald eine präparierte Seite im Browser aufgerufen wird. Die Antivirensoftware kann dies nicht verhindern.

**Acrobat-Reader**
Der Reader kann jeden beliebigen Code auf einem System ausführen, sobald ein präpariertes PDF-Dokument im Acrobat-Reader geöffnet wird. Die Antivirensoftware kann dies nicht verhindern, weil dies eine von Adobe vorgesehene und dokumentierte Funktion ist.

Derartige Vorkommnisse gibt es immer wieder und erfordern schnelles Handeln oder die Unterbindung des Internetzugriffs. Beiden Fällen ist gemeinsam, dass ohne Schutz die Kontrolle über den Rechner von einem Angreifer von außen übernommen werden kann, im zweiten Fall sogar besonders einfach.

### 3.3 Abhilfe nicht immer schnell möglich

Verschiedene Gründe verhindern, dass die erkannten Probleme zeitnah behoben werden können, somit bleiben die Risiken über längere Zeit bestehen.

**Keine Lösung verfügbar**
Beide Sicherheitslücken wurden im Internet ausgenutzt, über mehrere Tage/Wochen hinweg wurden von den Herstellern keine Updates zur Behebung zur Verfügung gestellt.

**Patchen nicht zeitnah möglich**
Die Aktualisierungs-Zyklen der automatischen Updates, sofern konfiguriert, greifen oft erst nach einigen Tagen, sodass selbst ein vorhandener Patch nicht zeitnah genutzt werden kann, es sei denn durch Bearbeiten jedes einzelnen Systems. Ohne übergreifendes Management der Rechner führt dies zu Ressourcen-Problemen.

**Kein zentrales Management vorhanden**
Im Fall von Adobe Acrobat konnte eine Umkonfiguration des Programms einen Angriff verhindern, ohne zentrales Management (AD, Zen-Works o. Ä.) muss jedes System einzeln von Hand behandelt werden. Ohne übergreifendes Management der Rechner führt dies zu Ressourcen-Problemen.

### 3.4 Absichern des Internet-Zugriffs durch Hinweis-Fenster

Künftig erscheint auf allen teilnehmenden Geräten bei Zugriff auf das Internet per Browser ein Hinweis, dass von diesem Gerät ein Internet-Zugriff nicht zulässig ist. Dieses Fenster wird vom WDR-Proxy erzeugt und vom Browser angezeigt.

### 3.5 Nutzung nach Authentifizierung mit der persönlichen Kennung

Ist ein administrativer Zugriff trotzdem zwingend notwendig, wird dieser nach Angabe von Nutzername/Passwort der persönlichen Kennung möglich. Damit wird der Zugriff für administrative Vorgänge nicht verhindert, sondern kontrolliert und bewusst ausgeführt. Funktionskennungen werden aufgrund der anonymen Nutzbarkeit nicht für das Verfahren zugelassen.

Auch sonst im Hintergrund ablaufende Aktualisierungen verbinden sich nach Authentifizierung mit dem Internet, da von den Proxys die IP-Adresse des Rechners und damit alle darauf laufenden Prozesse freigegeben werden. Der Zugang bleibt offen, bis festgestellt wird, dass für einen konfigurierbaren Zeitraum keine Aktivitäten stattgefunden haben. Der Zeitraum beträgt zunächst zehn Minuten.

### 3.6 Funktion nur nach Anforderung durch Systembetreiber

Jeder Systemverantwortliche kann seine Systeme für eine Teilnahme an der Maßnahme melden, es können jeweils ganze Netze berücksichtigt werden.

### 3.7 Anfälligkeit gegenüber Bedrohungen aus dem Internet wird minimiert

Da das Internet nach Umsetzung nicht mehr von Produktionssystemen aus genutzt wird, reduzieren sich die Bedrohungen stark. Zum Beispiel wird ein Angriff mit präparierten PDF-Dateien oder mit bösartigen Java-Applikationen verhindert.

Die Nutzung WDR-interner Angebote und webgestützter Systeme (Sendepläne, Dispo-Systeme usw.) bleibt wie gewohnt erhalten, hiervon gehen keine Gefahren aus.

Aufgrund der reduzierten Bedrohungen aus dem Internet reduziert sich die Notwendigkeit von Ad-hoc-Maßnahmen bei Bekanntwerden neuer Gefahren. Die notwendigen Update-Aktionen können zeitlich entspannter geplant und angegangen werden.

Für Administrationszwecke notwendige, kontrollierte Zugriffe auf vertrauenswürdige Seiten (z. B. Herstellerseiten für Updates) bergen nur ein geringes Risiko. Ohne Einschaltung weiterer Stellen (z. B. User Help Desk) zur Freigabe der Verbindung kann die Verbindung eigenständig zum Internet aufgebaut werden. Alle Verbindungen werden ebenso wie die normalen Zugriffe vom Arbeitsplatz-PC in den Proxys geloggt, zusätzlich wird noch die Kennung des Anwenders mitgeschrieben.

Automatische Verbindungen im Hintergrund ohne Kenntnis des Systembetreibers werden ebenfalls verhindert, eine Anmeldung mit Nutzername und Passwort ist den Applikationen in der Regel nicht möglich. Soll ein System regelmäßig auf das Internet zugreifen (Lizenzprüfung, Aktualisierung), so sind besondere Maßnahmen zu treffen.

### 3.8 Log-Dateien

Wie bisher werden alle Verbindungen zum Internet mit IP-Adresse des anfordernden PCs, Zeitstempel und angeforderten Inhalten protokolliert. Nach 90 Tagen werden die Daten gelöscht.

Alleine bei den Nutzern, welche aus Produktionsnetzen den Zugriff durch Authentifizierung freischalten, wird die Kennung (z. B. u4711) zusätzlich zu den bisherigen Daten mitgeschrieben. Das gilt nur für den Zugriff vom Produktionssystem aus. Alle weiteren Zugriffe dieser Nutzer werden wie bisher ohne Kennung protokolliert.

### 3.9 Datenschutz

Der Datenschutz ist durch die üblichen Vorkehrungen sichergestellt. Die Logdateien werden nach 90 Tagen gelöscht. Es haben nur die für das System zuständigen Administratoren Einblick in die Daten. Eine Herausgabe der Daten an Dritte ist nicht vorgesehen und erfolgt in Ausnahmefällen nur unter Einbeziehung der Hauptabteilung. Auf meine generellen Hinweise zur Dauer der Datenspeicherung (Punkt B 1.3) wird verwiesen. Die Höchstdauer der Speicherung sollte deutlich verkürzt werden.

# D Datenschutz beim Rundfunkgebühreneinzug

## 1. Gegenwärtige Situation

### 1.1 GEZ – Gebühreneinzugszentrale der öffentlich-rechtlichen Landesrundfunkanstalten

Als gemeinschaftlich von den öffentlich-rechtlichen ARD-Landesrundfunkanstalten, dem ZDF und dem DeutschlandRadio betriebenes Rechenzentrum mit Sitz in Köln erhebt, verarbeitet und nutzt die GEZ personenbezogene Teilnehmerdaten ausschließlich zum Zweck des Gebühreneinzugs. Der Gesetzgeber hat hier eine strikte Zweckbindung postuliert.

Da nach Angabe des Statistischen Bundesamtes 100 Prozent der Haushalte zumindest über ein Hörfunkgerät verfügen, sollte in jedem Haushalt auch ein Rundfunkteilnehmer gemeldet sein. Im Hinblick auf die Gebührengerechtigkeit versucht die GEZ zusammen mit den Rundfunkanstalten darum, möglichst alle Rundfunkteilnehmer zu erfassen.

Wichtige Instrumente hierfür sind der Beauftragtendienst der Rundfunkanstalten und sogenannte Mailingaktionen mit informativen Anschreiben an potenzielle Rundfunkteilnehmer und die breitflächige Erinnerung an die Rundfunkgebührenpflicht über Werbespots in Hörfunk und Fernsehen sowie Anzeigen in Printmedien.

Für die Kontrolle der GEZ sind die Datenschutzbeauftragten der einzelnen Rundfunkanstalten jeweils für ihren Teilnehmerkreis nach Maßgabe des für die Rundfunkanstalt geltenden Rechtes zuständig. Die Ausnahme bilden die Länder Berlin und Brandenburg (RBB), Bremen (RB) und Hessen (HR). Hier üben die Landesdatenschutzbeauftragten die Kontrollfunktion aus.

Die Daten der Rundfunkteilnehmer im Sendegebiet des WDR unterliegen ausschließlich der Kontrolle des Rundfunkbeauftragten für den Datenschutz beim WDR. Für ihn gelten die Vorschriften des Rundfunkgebührenstaatsvertrages, des WDR-Gesetzes und des Landesdatenschutzgesetzes Nordrhein-Westfalen.

Routinemäßige Datenschutzaufgaben im Bereich des Gebühreneinzugs werden gem. § 8 Abs. 2 Rundfunkgebührenstaatsvertrag von der internen Datenschutzbeauftragten der GEZ, Frau Kerstin Arens, vor Ort in Köln wahrgenommen. Mit ihr stehe ich in ständigem Austausch über datenschutzrechtliche Themen der GEZ und diesbezüglich zu treffende Maßnahmen. Als Mitglied des Arbeitskreises der Rundfunkdatenschutzbeauftragten ist sie in das Netzwerk der Kontrolle im Rundfunkbereich eingebunden. In ihrem jährlichen Bericht dokumentiert die Datenschutzbeauftragte ihre Beratungs-, Informations- und Überwachungstätigkeit und ist oft erster Ansprechpartner bei Datenschutzbeschwerden (datenschutz@gez.de).

### 1.2 Datenbestand bei der GEZ und beim WDR

Gegenwärtig umfasst der Gesamtdatenbestand bei der GEZ ca. 41,9 Mio. Teilnehmerkonten. Davon sind 3,0 Mio. Konten von gebührenbefreiten Teilnehmern.

Im Zuge der Einführung des Projektes BDONAB (Beauftragtendienst-Online-Abfrage), das den Rundfunkgebührenbeauftragten die Möglichkeit bietet, direkt auf die GEZ-Rundfunkteilnehmer-Datenbank zuzugreifen und Informationen zu den Teilnehmern ihres Gebietes über das Internet abzurufen, nutzen inzwischen die Hauptbeauftragten des WDR die Onlineverbindung mit der GEZ vom heimischen PC aus. Ein Datenaustausch ist hier nicht möglich, die Zugriffsmöglichkeiten beschränken sich auf die reine Datenabfrage. Ähnlich dem System BDONAB ist die Sammlung statistischer Daten der GEZ in Form des Rundfunkgebühren-Informationssystems (RGI) nur als Auskunftssystem für einen eingeschränkten Nutzerkreis der Gebührenabteilung zugänglich. Interaktionen sind auch hier nicht möglich.

Der WDR hat – auch aus Datenschutzgründen – davon Abstand genommen, die Nutzung des Systems durch die von den jeweiligen Hauptbeauftragten eingesetzten Unterbeauftragten über mobile Endgeräte vor Ort zuzulassen, etwas, was bei anderen Anstalten durchaus üblich ist. Maßgeblich für diese Entscheidung ist schlichtweg, dass bei einer Abfrage dieser sensiblen Daten direkt vor Ort, also beim potenziellen Rundfunkteilnehmer, die Vertraulichkeit der Daten trotz aller vertraglichen Verpflichtungen nicht vollständig gewährleistet werden kann.

### 1.3 Anfragen und Auskunftsersuchen

Sowohl bei der GEZ als auch beim WDR hat sich die Zahl der Anfragen und Auskunftsersuchen von Rundfunkteilnehmern in Datenschutzangelegenheiten im Wesentlichen auf gleichem Niveau gehalten. Die betriebliche Datenschutzbeauftragte der GEZ beantwortet im Auftrag der Datenschutzbeauftragten der einzelnen Landesrundfunkanstalten die an die GEZ gestellten Fragen zum Datenschutz im Rahmen des Gebühreneinzugs (sofern es sich nicht um Grundsatzfragen handelt). Eingaben aus dem WDR-Sendegebiet oder datenschutzrechtliche Grundsatzfragen, die über den Routineschriftwechsel hinausgehen, beantworte ich selbst.

Eine Reihe von Anfragen zum Datenschutz beim Rundfunkgebühreneinzug geht direkt bei mir ein oder werden von der Landesdatenschutzbeauftragten und vom Bundesdatenschutzbeauftragten zuständigkeitshalber an mich zur Bearbeitung weitergeleitet. Das Gros dieser Anfragen richtete sich gegen die Mailingmaßnahmen der GEZ zur Ermittlung von Rundfunkteilnehmern sowie den Beauftragtendienst. Mittelpunkt des Interesses bildet dabei die Herkunft der gespeicherten Daten und die grundsätzliche Berechtigung zur Datenerhebung. Auch die Zahl der Bitten um Sperrung, Löschung oder Berichtigung der gespeicherten Daten zeigt eine leicht steigende Tendenz. Vielfach werden für

Anfragen standardisierte Schreiben verwendet, die auf Internetseiten mit Anti-GEZ-Tenor als Mustervorlage für den »Kampf« mit der GEZ bereitstehen.

Jahrelang kam die überwiegende Mehrzahl der Anfragen von Finanzämtern und Kommunalkassen, die sich die Preisgabe von Adressen und Bankverbindungen der Rundfunkteilnehmer erhofften. Mit dem Hinweis auf die strenge Zweckbindung der Teilnehmerdaten an den Rundfunkgebühreneinzug (vgl. § 3 Abs. 3 Rundfunkgebührenstaatsvertrag) wurden und werden diese Auskunftsersuchen konsequent abgelehnt. Durch das »Gesetz zur Förderung der Steuerehrlichkeit« vom 23. Dezember 2003 (BGBl. 2003, 2928) ist in Art. 2 auch eine Änderung der Abgabenordnung vorgenommen worden. So erhielt insbesondere § 93 AO eine Ergänzung um einen Absatz 7, der Finanzbehörden erlaubt, über das Bundesamt für Finanzen bei den Kreditinstituten einzelne Daten abzurufen. Nach § 93 b AO kann dies sogar automatisiert geschehen. Die neue gesetzliche Regelung ist zwar einerseits ein Schritt auf dem Weg zum gläsernen Bankkunden, führte andererseits jedoch zu einem deutlichen Rückgang (von 577 Anfragen im Jahr 2004 auf 157 im Jahr 2007) der Auskunftsbegehren öffentlicher Stellen bei der GEZ. Im Sendebereich des WDR hat es seit 2007 gar keine Anfrage mehr gegeben.

### 1.4 Mailing – ein Dauerbrenner

Als Dauerthema gab das sogenannte Mailing der GEZ auch im Berichtszeitraum wiederholt Anlass zur kritischen Betrachtung aus der Sicht des Datenschutzes, obwohl das Verfahren unbestritten für die Ausschöpfung des Teilnehmerpotenzials von großer Bedeutung ist. Da eine beachtliche Zahl der Rundfunkteilnehmer aus den unterschiedlichsten Gründen es versäumt, Rundfunkempfangsgeräte anzumelden, ist es nicht zuletzt im Sinne höherer Gebührengerechtigkeit wichtig, das entsprechende Potenzial zu heben. Das Instrument »Direct-Mailing« ist hierbei unumgänglich und erfolgreich. Mehrmals im Jahr startet die GEZ Aktionen mit informativen Anschreiben über die Regelungen der Gebührenpflicht und der Aufforderung, dieser auch nachzukommen.

Die dafür verwendeten Adressen stammen entweder aus den regelmäßig übermittelten Adressdaten der Einwohnermeldebehörden nach den melderechtlichen Vorschriften der einzelnen Bundesländer (EMA-Mailing) oder es werden Adressen bestimmter Zielgruppen (z. B. Leser von Fernsehzeitschriften, junger Erwachsener) von gewerblichen Adresshändlern angemietet. Die Adressdaten werden mit dem Teilnehmerbestand der GEZ abgeglichen. Finden sich die Adressdaten nicht im Datenbestand der GEZ wieder, wird an die Rundfunkgebührenpflicht erinnert, da statistisch gesehen 100 Prozent der Haushalte zumindest über ein Hörfunkgerät verfügen.

Der GEZ-Geschäftsbericht für das Jahr 2009 verzeichnet 6,3 Mio. angeschriebene Adressen mit einem Rücklauf von 4,5 Mio. Antwortschreiben und daraus resultierenden neuen Anmeldungen bzw. Zumeldungen in Höhe von 11 Prozent. Diese hohe Erfolgsquote deckt die Kosten für insgesamt 16,6 Mio. versandte Briefen (Erst- und Erinnerungsschreiben) bei Weitem.

Obwohl der Adresshandel in der Bundesrepublik Deutschland nach den geltenden Datenschutzgesetzen zulässig ist, wurde die Praxis der GEZ, auf Daten der privaten Adresshändler zurückzugreifen, vielfach angegriffen. Die bundesweiten Diskussionen um die Rechtmäßigkeit der Adressanmietung ebbten erst mit der einheitlichen Rechtsnorm des zu erlassenden § 8 Abs. 4 Rundfunkgebührenstaatsvertrag ab. Die Modifizierung dieser Vorschrift im Rahmen des 10. Rundfunkänderungsstaatsvertrages erfolgte gemeinsam durch die Rundfunkreferenten der Länder, die Landesdatenschutzbeauftragten sowie den Rundfunkdatenschutzbeauftragten.

Der Abgleich vor allem der angemieteten Adressen führt immer wieder zu kuriosen Ergebnissen. Vor allem bei ausländischen Rundfunkteilnehmern kann es mitunter zu Verwechslungen von Vor- und Zunamen kommen, sodass redliche Gebührenzahler zu erneuter Anmeldung aufgefordert werden. Auch Namen von längst Verstorbenen tauchen unter den Adressen auf und führen zu peinlichen Anschreiben. Obwohl auf Drängen der Datenschutzbeauftragten die Jugendlichen unter 18 Jahre von Mailingmaßnahmen ausgenommen sind, unterlaufen auch hier Fehler durch Erwerb mangelhafter Adressen, trotz vertraglicher Zusicherung der Volljährigkeit der Adressaten. Auch die Texte der informativen Anschreiben selbst sind auf dem datenschutzrechtlichen Prüfstand als korrekturbedürftig befunden worden. Zur Einhaltung der Formalien im Sinne des Datenschutzes muss nicht nur auf die zugrunde liegenden Gesetze hingewiesen werden und auf die Pflicht zur Auskunftserteilung auf die Anschreiben, sondern ebenso auf die Freiwilligkeit der Antwort in den ganz besonderen Fällen, wenn tatsächlich keinerlei Rundfunkempfangsgeräte, auch keine neuartigen, vorhanden sind. Diese Voraussetzungen werden inzwischen – was auch bereits obergerichtlich bestätigt wurde – erfüllt.

Sämtliche Adressen aus Mailingmaßnahmen werden nach Bearbeitung des Rücklaufs aus den Aktionen gelöscht und für keinen anderen Zweck als für die jeweilige Aktion, für die sie erworben wurden, verwendet. Nach der datenschutzrechtlichen Vorgabe der strengen Zweckbindung von Daten dürfen auch keine Zuschauer- bzw. Zuhöreradressen aus Programmaktionen für Mailingmaßnahmen der GEZ herangezogen werden.

Im Falle des Inkrafttretens des Rundfunkbeitragsstaatsvertrages sind im privaten Bereich bis 31. Dezember 2014 Mailingmaßnahmen unter Nutzung kommerziellen Adressmaterials untersagt (§ 14 Abs. 10).

## 2. Vorbereitung der Umsetzung der Neuregelungen im Rundfunkbeitragsstaatsvertrag

Zur Vorbereitung der Maßnahmen, die zur Umsetzung der sich aus dem neuen Rundfunkbeitragsstaatsvertrag ergebenden Änderungen erforderlich sind, ist bei der GEZ ein Controlboard eingerichtet worden, dem ich als Datenschutzbeauftragter auch für den Arbeitskreis der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten angehöre. Im Rahmen der von der GEZ für die Rundfunkanstalten umzusetzenden Maßnahmen, die zum Großteil im Hinblick auf die Übergangsvorschrift des § 14 Rundfunkbeitragsstaatsvertrag vor einer Ratifizierung zum 1. Januar 2012 greifen müssen, ist auch der Sicherstellung datenschutzrechtlicher Belange vollumfänglich Rechnung zu tragen.

Insoweit kann ich festhalten, dass die Verantwortlichen innerhalb der GEZ Datenschutzbelange vollumfänglich berücksichtigen.

Es gab lediglich einige Feinjustierungen, auf die ich aufmerksam machen musste, die aber nunmehr auch umgesetzt werden:

1. Es war in Erwägung gezogen worden, bei den Betriebsstätten die Zahl aller vorhandenen Fahrzeuge zu erheben und auch auf Dauer zu speichern. Insoweit musste ich auf die Bestimmung des § 8 Abs. 4 Nr. 12 des Rundfunkbeitragsstaatsvertrages hinweisen, wonach nur die Anzahl und der Zulassungsort der beitragspflichtigen Kraftfahrzeuge erhoben und gespeichert werden darf. Die Erhebung nicht beitragspflichtiger Kfz-Daten ist unzulässig. Dem wurde zwischenzeitlich Rechnung getragen.

2. Im Rahmen der Übergangsregelungen des § 14 Abs. 2 Rundfunkbeitragsstaatsvertrag müssen alle als nicht private Rundfunkteilnehmer gemeldeten natürlichen oder juristischen Personen ab 1. Januar 2012 angeschrieben werden und auf ihre Verpflichtung hingewiesen werden, alle Tatsachen anzuzeigen, die Grund und Höhe der Beitragspflicht ab dem 1. Januar 2013 betreffen. Insoweit wurden bei der GEZ Anschreiben und jeweils zwei Erinnerungsbriefe entwickelt, wobei die Erinnerungsbriefe jeweils deutlicher auf die bestehende Verpflichtung hinweisen. Außerdem fand sich in den Erinnerungsbriefen der Hinweis, dass das Nichtnachkommen der Verpflichtung eine Ordnungswidrigkeit nach § 12 Abs. 1 Nr. 2 Rundfunkbeitragsstaatsvertrag darstellt.

   Dieser Hinweis wurde, auch auf meine Anregung hin, gestrichen. Denn Tatsache ist, dass die Vorschrift des § 12 erst zum 1. Januar 2013 in Kraft tritt. Somit kann derjenige, der seiner Verpflichtung, bereits im Jahre 2012 die erforderlichen Angaben zu machen, nicht nachkommt, jedenfalls im Jahre 2012 nicht wegen einer Ordnungswidrigkeit belangt werden.

   Auch dem wurde Rechnung getragen.

3. Es wurde seitens der GEZ der Wunsch geäußert, insbesondere bei Namensverschiedenheit zu einer konkreten Wohnung nicht nur den zur Zahlung herangezogenen Beitragsschuldner zu speichern, sondern auch die übrigen volljährigen Bewohner einer Wohnung. Als Grund wurde angegeben, dass nur dann sichergestellt werden kann, dass im Rahmen von Mailingaktionen, die 2015 wieder aufgenommen werden können, solche Personen nicht unnötig angeschrieben werden. Auf diese Weise sollten Irritationen bei den Teilnehmern vermieden werden.

   So nachvollziehbar die Gründe auch sein mögen, die Regelungen des Rundfunkbeitragsstaatsvertrages sind insoweit eindeutig, als nur die Person des zahlungspflichtigen Beitragsschuldners gespeichert werden darf. Für die Speicherung der Daten weiterer Personen in einer Wohnung gibt es keine gesetzliche Grundlage.

# Schlussbemerkung

Der Bericht behandelt meine datenschutzrechtliche Beratungs- und Prüftätigkeit im Wesentlichen im WDR und in der GEZ.

Über die beträchtliche Ausweitung geltender Gesetze und Erlass neuer Gesetze mit datenschutzrechtlichen Bestimmungen, die für eine Entscheidung über die Zulässigkeit einer Datenerhebung oder -verarbeitung von Bedeutung sind, hatte ich in meinem letzten Tätigkeitsbericht ebenso berichtet wie über den aufkommenden Wunsch von Behörden und Staatsorganen zum Aufbau umfangreicher Datensammlungen unter dem Aspekt einer wirksamen Terrorismusbekämpfung. Hier ist nach wie vor darauf zu achten, dass die Tendenz, Überwachungsmechanismen zu intensivieren, die Persönlichkeitsrechte der Bürgerinnen und Bürger nicht in einem nicht vertretbaren Maß hintanstehen lässt. Soweit ist auch darauf hinzuweisen, dass in einigen Fällen erst das Bundesverfassungsgericht den Persönlichkeitsrechten des Einzelnen wieder die ihm zukommende Bedeutung zukommen lassen musste und wohl auch noch zukommen lassen muss.

Zusammengefasst ist es weiterhin so, dass für den WDR zwar vornehmlich eine positive Bilanz gezogen werden kann. Andererseits darf aber nicht übersehen werden, dass der Datenschutz und damit auch der Schutz der Persönlichkeitsrechte eine ständige Aufgabe mit immer neuen Herausforderungen und Anfechtungen sind.

Aus diesem Grunde sehe ich es nach wie vor in hohem Maße als erforderlich an, im WDR und seiner Darstellung nach außen die Bedeutung des Datenschutzes zu unterstreichen. In gleichem Maße richtet sich diese Forderung aber auch an ein verantwortliches Verhalten der Mitarbeiterinnen und Mitarbeiter des WDR im Umgang mit personenbezogenen Daten.

Nach wie vor darf auch nicht übersehen werden, dass der Beauftragte für den Datenschutz – auch bei der vorhandenen Personalausstattung mit einem Mitarbeiter und einer Halbtagssekretärin – an die Kapazitätsgrenzen für eine umfassende Kontrolle und insbesondere Beratung der betroffenen Bereiche stößt, zumal er nach § 53 Abs. 2 Satz 2 WDR-Gesetz auch andere Aufgaben im WDR wahrnimmt, die ihrerseits eine fast 100-prozentigen Auslastung beinhalten.

Hier ist in der Tat zu überlegen, ob nicht – wie etwa beim Mitteldeutschen Rundfunk – der Beauftragte für den Datenschutz von der Wahrnahme weiterer Aufgaben im WDR entbunden werden kann. Dies würde darüber hinaus die unabhängige Stellung des Datenschutzbeauftragten zusätzlich unterstreichen.

Von den angesprochenen Einzelbemerkungen abgesehen, bleibt zusammenfassend aber auch dieses Mal festzuhalten, dass sich bei meiner Prüfung des Datenschutzes und der Datensicherheit im WDR und in der GEZ keine datenschutzrechtlichen Beanstandungen nach § 53 Abs. 3 WDR-Gesetz ergeben haben.

Köln, 20. Juni 2011

**Thomas Drescher**
Datenschutzbeauftragter des WDR

Herausgeber:
Westdeutscher Rundfunk Köln
Marketing

Datenschutzbeauftragter:
Thomas Drescher

Gestaltung:
www.mohrdesign.de

Foto: Mauritius

Juli 2011