



Körperschaft des öffentlichen Rechts

Achter Tätigkeitsbericht
des Beauftragten für den Datenschutz

Berichtszeitraum
1. Oktober 2007 - 30. September 2009

Inhaltsverzeichnis

A. Vorbemerkung	4
B. Aufgaben und Stellung des Beauftragten für den Datenschutz im Deutschlandradio	5
C. Entwicklung des Datenschutzrechts	7
I. Bundesdatenschutzgesetz	7
1. Auswirkungen auf Direktmarketing und Adresshandel	8
2. Auftragsdatenverarbeitung	10
3. Datenschutz im Arbeitsverhältnis	10
4. Informationspflicht bei unrechtmäßiger Kenntniserlangung durch Dritte	11
5. Weitere Neuerungen	12
D. Datenschutz beim Deutschlandradio	13
I. Ausstattung mit eigenen finanziellen Mitteln	13
II. Veröffentlichung des Datenschutzberichts	13
III. Aktuelle Vorgänge im Berichtszeitraum	14
1. Speicherung von IP-Adressen	14
2. Videoüberwachung	16
a) Funkhaus Köln	16
b) Funkhaus Berlin	17
c) Dienstvereinbarung Videoüberwachung	18
3. Aufzeichnung von Personal- und Redakteursversammlungen	18
a) Personalversammlung	19
b) Redakteursversammlung	20
4. Automatische Aufzeichnung eingehender Anrufe	21
5. Speicherung von Hörertelefonnummern	23
6. Einsatz von sog. Referrern	23

E. Datenschutz bei der GEZ	24
F. IVZ	25
G. Informationsaustausch	25
I. KIT-Sitzungen	25
II. AK-DSB	26

A. Vorbemerkung

Der Beauftragte für den Datenschutz erstattet nach § 18 Abs. 7 des Staatsvertrages über die Körperschaft des öffentlichen Rechts „Deutschlandradio“ (Deutschlandradio-Staatsvertrag – DRadio-StV –) dem Verwaltungsrat alle zwei Jahre einen Bericht über seine Tätigkeit.

Der achte Tätigkeitsbericht schließt an den siebten Bericht für den Zeitraum vom 1. Oktober 2007 bis 30. September 2009 an.

In dem vorliegenden Bericht werden allgemeine Entwicklungen des Datenschutzes sowie datenschutzrechtlich relevante Veränderungen und Problemstellungen innerhalb des Deutschlandradios während des Berichtszeitraums dargestellt. Förmliche Beanstandungen, die in dem Verfahren nach § 18 Abs. 5 DRadio-StV hätten bearbeitet werden müssen (Beanstandung beim Intendanten und gleichzeitige Unterrichtung des Verwaltungsrats), waren im Berichtszeitraum nicht auszusprechen.

Herr Dr. Markus Robak ist auf der Sitzung des Verwaltungsrates vom 8. November 2007 für vier Jahre zum Beauftragten für den Datenschutz des Deutschlandradios bestellt worden. Herr Dr. Robak ist zum 14. Juni 2009 aus dem Dienst des Deutschlandradios ausgeschieden und hat den vorliegenden Bericht für den Zeitraum bis zu diesem Datum erstellt. Der Unterzeichner ist auf der Sitzung des Verwaltungsrates vom 15. Juli 2009 für 4 Jahre zum Beauftragten für den Datenschutz des Deutschlandradios bestellt worden. Der vorliegende Bericht stammt für den nach dem Ausscheiden des Herrn Dr. Robak verbleibenden Berichtszeitraum vom 15. Juni bis 30. September 2009 von dem Unterzeichner.

Sowohl Herr Dr. Robak als auch der Unterzeichner haben die Aufgaben des Datenschutzbeauftragten neben ihrer jeweiligen Beschäftigung im Justitiariat bzw. als Justitiar des Deutschlandradios wahrgenommen.

B. Aufgaben und Stellung des Beauftragten für den Datenschutz im Deutschlandradio

Nach § 18 Abs. 3 DRadio-StV überwacht der Beauftragte für den Datenschutz die Einhaltung der Datenschutzvorschriften des DRadio-StV, des Bundesdatenschutzgesetzes (BDSG) und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit der Körperschaft.

Aufgrund § 17 DRadio-StV gilt das BDSG bei der Verarbeitung von personenbezogenen Daten zu eigenen journalistischen oder literarischen Zwecken nur eingeschränkt in Bezug auf das Datengeheimnis und die Datensicherung (sog. „Medienprivileg“). Diese eingeschränkte Geltung beruht auf der grundgesetzlich geschützten Presse- und Rundfunkfreiheit und soll die redaktionelle Sammlung von personenbezogenen Daten ermöglichen. Soweit die Rundfunkanstalten dagegen personenbezogene Daten von Rundfunkteilnehmerinnen und -teilnehmern oder Mitarbeiterinnen und Mitarbeitern für Verwaltungszwecke verarbeiten, unterliegen sie in vollem Umfang den Bestimmungen der Datenschutzgesetze, hier dem BDSG.

In Ausübung seines Amtes ist der Beauftragte für den Datenschutz nach § 18 Abs. 2 DRadio-StV unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Verwaltungsrates. Nach § 16 DRadio-StV sind die Vorschriften des BDSG entspre-

chend anzuwenden. Gemäß § 16 DRadio-StV i. V. m. § 4g BDSG und § 18 DRadio-StV ergeben sich folgende Aufgaben:

Kontrolle aller Bereiche, die personenbezogene Daten verarbeiten;

Mitwirkung bei der Planung von Vorhaben, die der automatisierten Verarbeitung von Daten dienen;

Schulung von Mitarbeitern im Bereich Datenschutz;

Beanstandung von Verstößen gegen datenschutzrechtliche Bestimmungen oder sonstigen Mängeln bei der Verarbeitung personenbezogener Daten bei dem Intendanten, verbunden mit der Aufforderung zur Behebung der Verstöße oder Mängel;

Untersuchung von Beanstandungen von betroffenen Mitarbeiterinnen oder Mitarbeitern bzw. Dritter.

Der Aufgabenkatalog verdeutlicht, dass der Beauftragte für den Datenschutz an die Stelle eines staatlichen Datenschutzbeauftragten tritt. Er tut dies im gesamten Aufgabenbereich der Körperschaft. Es liegt also keine „gespaltene Zuständigkeit“ vor wie bei verschiedenen Landesrundfunkanstalten, bei welchen der Rundfunkdatenschutzbeauftragte nur im Bereich des Redaktionsdatenschutzes an die Stelle des staatlichen Landesdatenschutzbeauftragten tritt. Er prüft, ob die betrieblich Verantwortlichen die Bestimmungen des Datenschutzes beachten und leistet Hilfestellung.

Er nimmt nicht die Aufgaben eines betrieblichen Datenschutzbeauftragten i. S. d. § 4f BDSG wahr. Es gehört daher nicht zu seinen Aufgaben, für die betriebsinterne Organisation des Datenschutzes und für die Einhaltung der einschlägigen Bestimmungen zu sorgen. Diese Aufgabe obliegt vielmehr dem Intendanten als oberstem Dienstherrn bzw. den von ihm beauftragten Personen bzw. Stellen.

C. Entwicklung des Datenschutzrechts

Im Folgenden soll ein kurzer allgemeiner Überblick über Entwicklungen im Bereich des Datenschutzrechts im Berichtszeitraum gegeben werden.

I. Bundesdatenschutzgesetz

Der Bundestag hat am 3. Juli 2009 die sog. Novelle II des Bundesdatenschutzgesetzes (BDSG) verabschiedet. Obwohl die beschlossenen Änderungen am Ende nicht derart gravierend ausgefallen sind, wie noch im Gesetzesentwurf der Bundesregierung vom 18. Februar 2009 vorgesehen, sieht die Novelle doch einige sehr bedeutsame Neuerungen insbesondere bei der Datennutzung für Werbung und Marketing vor, die von Unternehmen zukünftig zu beachten und umzusetzen sind. Die Änderungen sind größtenteils am 1. September 2009 in Kraft getreten.

1. Auswirkungen auf Direktmarketing und Adresshandel

Besonders umstritten war die zunächst vorgesehene Abschaffung des sog. Listenprivilegs. Danach dürfen Unternehmen bestimmte, in Listen oder sonst zusammengefasste Daten (u. a. Name, Beruf und Anschrift ihrer Kunden) an Dritte für deren Werbezwecke weitergeben und selbst solche Adresslisten für eigene Marketingmaßnahmen von Dritten beziehen, ohne dass eine Einwilligung der Betroffenen vorliegen muss (§ 28 Abs. 3 Satz 1 Nr. 3 BDSG a. F.). Dieses Privileg erlaubt auch den gewerbsmäßigen Adresshandel (§ 29 Abs.

2 Satz 1 Nr. 1b BDSG a. F.) sowie die Datennutzung für die Markt- und Meinungsforschung.

Das Listenprivileg ist durch die Novelle beschränkt worden (§ 28 Abs. 3 Satz 2 BDSG n. F.). Das werbende Unternehmen darf unter das Privileg fallende Daten, die es selbst beim Betroffenen (z.B. bei der Warenbestellung seines Kunden) oder aus allgemein zugänglichen Quellen, etwa dem Internet, erhoben hat, für eigene Werbezwecke verwenden. Zulässig – und großzügiger geregelt als die Eigenwerbung – ist unter dem Listenprivileg auch die Geschäftswerbung, d.h. Werbung mit Bezug zur beruflichen Tätigkeit des Betroffenen unter dessen geschäftlicher Anschrift sowie die Spendenwerbung.

Ebenso bleibt nach der neuen Gesetzeslage der Handel mit Adresslisten grundsätzlich möglich. Allerdings ist der Adresshändler ebenso wie jedes andere Unternehmen, das Adressen an Dritte weitergibt, nunmehr gesetzlich verpflichtet, die Herkunft und den Empfänger der Daten für zwei Jahre zu speichern und den Betroffenen auf Verlangen entsprechend Auskunft zu erteilen (§ 28 Abs. 3 Satz 4 i. V. m. § 34 Abs. 1a BDSG n. F.). Wer solche Fremddaten für Werbezwecke nutzt, muss nun ferner in der Werbung eindeutig angeben, wer die Daten erstmalig erhoben hat (§ 28 Abs. 3 Satz 4 BDSG n. F.). Es ist anzunehmen und vom Gesetzgeber beabsichtigt, dass die Bereitschaft zum Verkauf eigener Kundendaten zurückgehen wird.

Unabhängig von den Voraussetzungen des Listenprivilegs bleibt die Werbung für fremde Angebote in Form von sog. Beipack- und Empfehlungswerbung (z.B. fügt eine Bank ihrer Werbung an eigene Kunden das Angebot eines Verlages für ein Zeitungsabonnement bei) zulässig (§ 28 Abs. 3 Satz 5 BDSG n. F.).

Schließlich gelten die Einschränkungen des Listenprivilegs in gleicher Weise für den geschäftsmäßigen Adresshandel (§ 29 BDSG n. F.), während die geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- und Meinungsforschung nunmehr gesondert in einem neuen § 30a BDSG n. F. geregelt ist.

Die dargestellten Änderungen sind am 1. September 2009 in Kraft getreten; es gilt jedoch eine Übergangsregelung: Bestandsdaten, die vor dem 1. September 2009 erhoben oder gespeichert worden sind, können nach § 47 BDSG n. F. weiterhin auf der Grundlage des bisherigen Rechts für Zwecke der Markt- oder Meinungsforschung noch bis zum 31. August 2010 sowie für Werbezwecke bis zum 31. August 2012 verarbeitet und verwendet werden. Demgegenüber müssen für die Datenerhebung und -speicherung ab dem 1. September 2009 die neuen strengeren Vorschriften eingehalten werden.

2. Auftragsdatenverarbeitung

Die Novelle des BDSG bringt Änderungen für die Auftragsdatenverarbeitung. Nach § 11 Abs. 2 Satz 2 BDSG n. F. sind künftig im Vertrag mit dem beauftragten Dienstleister mindestens die zehn im Gesetz aufgelisteten Punkte zu regeln, andernfalls begeht der Auftraggeber eine bußgeldbewehrte Ordnungswidrigkeit (§ 43 Abs. 1 Nr. 2b BDSG n. F.). Bestehende Vertragsverhältnisse mussten den neuen gesetzlichen Anforderungen spätestens bis zum 1. September 2009 angepasst werden.

3. Datenschutz im Arbeitsverhältnis

Durch die BDSG-Novelle ist eine spezielle Vorschrift zum Datenschutz im Arbeitsverhältnis eingeführt worden, die die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Beschäftigten erlaubt, wenn dies für die Einstellungsentscheidung sowie später für die Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG n. F.).

Eingeschränkt wird die Möglichkeit der Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten zum Zwecke der Korruptionsbekämpfung und Aufdeckung sonstiger Straftaten (§ 32 Abs. 1 Satz 2 BDSG n. F.). Erforderlich sind tatsächliche Anhaltspunkte, die den Verdacht der Begehung einer Straftat im Beschäftigungsverhältnis begründen; Massenscreenings großer Teile der Belegschaft etwa zur Korruptionsbekämpfung sind damit ausdrücklich ausgeschlossen. Ferner muss die Datenerhebung und -nutzung zur Aufdeckung erforderlich sein, und schließlich darf das entgegenstehende Interesse des Beschäftigten nicht überwiegen, wobei die Art und die Schwere der Straftat zu berücksichtigen sind.

§ 32 Abs. 2 BDSG n. F. regelt ferner, dass der Arbeitnehmerdatenschutz auch bei nicht automatisierter und nicht dateigebundener Datenverarbeitung gilt und somit z.B. händisch geführte Personalakten erfasst. Schließlich gilt nun für betriebliche Datenschutzbeauftragte ein besonderer Kündigungsschutz, § 4f Abs. 3 Satz 5 bis 7 BDSG n. F.

4. Informationspflicht bei unrechtmäßiger Kenntniserlangung durch Dritte

Das neue BDSG sieht in § 42a eine an dem US-amerikanischen Recht entlehnte Informationspflicht des für die Datenverarbeitung verantwortlichen Unternehmens vor. Diese greift, wenn gespeicherte, besonders sensible Daten unrechtmäßig an Dritte übermittelt oder diesen anderweitig bekannt werden und daraus schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Die Pflicht beschränkt sich auf bestimmte personenbezogene Daten, wie z.B. Angaben über den Gesundheitszustand und die politische Einstellung, Informationen, die einer beruflichen Schweigepflicht z.B. von Rechtsanwälten unterliegen, Daten über Straftaten und Ordnungswidrigkeiten, Konto- und Kreditkartennummern sowie Daten, die bei der Nutzung von Online- und Telekommunikationsdiensten gespeichert werden.

Benachrichtigt werden müssen die zuständige Aufsichtsbehörde sowie die Betroffenen. Für solche Benachrichtigungen, die letztlich einer Selbstanzeige gleichkommen, gilt ein Verwertungsverbot im Straf- bzw. Ordnungswidrigkeitsverfahren. Wird eine Benachrichtigung sämtlicher Betroffenen mit vertretbarem Aufwand – insbesondere aufgrund ihrer Vielzahl – unmöglich, so kann das Unternehmen stattdessen die Betroffenen durch halbseitige Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen informieren. Ein Verstoß gegen die Informationspflicht stellt eine Ordnungswidrigkeit dar (§ 43 Abs. 2 Nr. 7 BDSG n. F.).

5. Weitere Neuerungen

In § 38 Abs. 5 BDSG n. F. werden die Befugnisse der Aufsichtsbehörden bei der Feststellung von Datenschutzverstößen dahingehend erweitert, dass sie konkrete Maßnahmen zu deren Beseitigung anordnen können.

Der Katalog der Ordnungswidrigkeiten in § 43 BDSG wird erweitert, die Bußgeldgrenzen von bislang 25.000 € bzw. 250.000 € auf 50.000 € bzw. 300.000 € erhöht und in § 43 Abs. 3 Satz 2 und 3 BDSG n. F. das Instrument der Gewinnabschöpfung eingeführt.

Das Datenschutzauditgesetz wurde dagegen nicht verabschiedet.

D. Datenschutz beim Deutschlandradio

I. Ausstattung mit eigenen finanziellen Mitteln

Seit dem Wirtschaftsjahr 2005 verfügt der Datenschutzbeauftragte über ein eigenes bescheidenes Budget, aus dem die für sein Amt anfallenden Kosten für z.B. Reisen, externe Beratungen und Literatur abgedeckt werden können. Diese Ausstattung mit eigenen Mitteln soll die Unabhängigkeit des Datenschutzbeauftragten, wie sie durch den Staatsvertrag vorgegeben ist, unterstützen.

II. Veröffentlichung des Datenschutzberichts

Der Datenschutzbericht wird im Internetangebot des Deutschlandradios unter der Adresse www.dradio.de/wir/datenschutz veröffentlicht. Er ist von der Homepage über den Link „Wir über uns“ erreichbar.

III. Aktuelle Vorgänge im Berichtszeitraum

Im Berichtszeitraum war der Datenschutzbeauftragte mit einer Vielzahl von Einzelvorgängen befasst, die in Anfragen zum Datenschutz, in Kontrollen bereits bestehender datenschutzrelevanter Abläufe und auch in der Beteiligung in der Planungsphase solcher Vorgänge bestanden. Einzelne Vorgänge sollen im Folgenden kurz angesprochen werden.

1. Speicherung von IP-Adressen

Ein regelmäßiger Nutzer von dradio.de meldete sich bei dem Datenschutzbeauftragten und begehrte Auskunft, ob das Deutschlandradio die IP-Adresse der Besucher von dradio.de speichere und, falls ja, wie lange. Nach Einschätzung des Datenschutzbeauftragten stand hinter dieser Anfrage kein ernstes Interesse an einer Antwort, sondern sie sollte offensichtlich als ein Hinweis auf ein Urteil des Amtsgerichts Berlin Mitte (s. u.) zu dem Thema dienen. Der Betreffende war Inhaber eines E-Mail Accounts bei der Universität Bremen und besuchte von dort auch die Seiten von dradio.de.

Es gehört zum Standard der IT-Sicherheit von Internet-Angeboten, dass der Betreiber temporär Daten von Besuchern seiner Seiten speichert, um insbesondere Angriffe auf die Funktionalität und Stabilität des Systems erkennen und abwehren zu können. Zu den üblicherweise gespeicherten Daten gehört die IP-Adresse des Nutzers.

Es gibt statische und dynamische IP-Adressen. Letztere werden von Internet-Providern an ihre Kunden für die Dauer eines Internetbesuchs vergeben. Der Kunde erhält eine IP-Adresse zugewiesen, die gerade frei ist. Bei jedem Internetzugang erhält ein Kunde im Zweifel eine andere IP-Adresse zugewiesen.

Datenschutzrechtlich ist seit langem umstritten, ob dynamische IP-Adresse als personenbezogene Daten im Sinne des Datenschutzrechts anzusehen sind, da sie einem bestimmten Nutzer nur dann zugeordnet werden können, wenn der Provider eine entsprechende Auskunft erteilt.

In einem Urteil des Amtsgerichts Berlin-Mitte vom 27.03.2007 (AZ 5 C 314/06) bezog der Richter – soweit ersichtlich erstmalig in der deutschen Rechtsprechung – die Position, dynamische IP-Adressen seien personenbezogene Daten. Diese Entscheidung hat in der Internet-Gemeinde für Aufsehen gesorgt, denn sie beurteilt eine gängige Praxis zahlloser Diensteanbieter als rechtswidrig. Sie ist allerdings keine Grundsatzentscheidung, die zwingend von jedermann berücksichtigt werden muss. Tatsächlich wird das Urteil sehr kontrovers diskutiert, und obwohl sich auch das Landgericht Berlin in zweiter Instanz mit dem Fall befasst hat, war die entscheidende Frage – gehören IP-Adressen zu den personenbezogenen Daten? – dort nicht mehr zum Gegenstand des Verfahrens. Tatsächlich hat zwischenzeitlich das Amtsgericht München die gegenteilige Position bezogen (Urteil vom

30.09.2008 – 133 C 5677 /08). Es bleibt also abzuwarten, wie in Zukunft ein Obergericht entscheiden wird.

Der Datenschutzbeauftragte hat dem Auskunftsbegehren des o. g. Nutzers nicht entsprochen. Er konnte die Frage des Personenbezugs von dynamischen IP-Adressen offenlassen, da aus seiner Sicht der Nutzer über eine IP-Adresse der Universität Bremen im Internet surfte. Daher war nicht ersichtlich, dass diese IP-Adresse einen Personenbezug zu dem Betroffenen ermöglicht hätte.

2. Videoüberwachung

Schon im vorangegangenen Berichtszeitraum hatte der seinerzeitige Datenschutzbeauftragte (Herr Dr. Stefan Frank) die Videoüberwachung in den beiden Funkhäusern geprüft und darüber Bericht erstattet. Im nun abgelaufenen Berichtszeitraum hat der Datenschutzbeauftragte die Videoüberwachung ebenfalls geprüft und ist dabei im Wesentlichen zu denselben Ergebnissen wie sein Vorgänger gekommen.

a) Funkhaus Köln

Die Videoüberwachung durch eine Kamera (Nr. 8) vor dem Haupteingang wurde erneut als unzulässig angesehen, da sie einen Bereich betrifft, der unmittelbar vom Empfang kontrolliert werden kann (diese Einschätzung stammt aus der Zeit vor den baulichen Änderungen des Eingangsbereichs).

Der Datenschutzbeauftragte hielt die Videoüberwachung durch drei Kameras (Nr. 13, 14 und 15) im Bereich Zufahrt Tiefgarage nicht für erforderlich, wenn und solange das Schrankenhäuschen an der Zufahrt zur Tiefgarage durch eine/n Pförtner/in besetzt ist.

Schließlich wurde der Standort von zwei weiteren Kameras (Nr. 3 und 4) im Aufgang von der Tiefgarage in das Funkhaus beanstandet, weil der Datenschutzbeauftragte deren Nutzen als äußerst gering und die Eingriffsqualität und vor allem -quantität an der Stelle als sehr hoch einschätzte.

Die übrigen Kameras sind nach Auffassung des Datenschutzbeauftragten zulässig, wenn sie nur ereignisbezogen und für kurze Zeit aufzeichnen.

b) Funkhaus Berlin

Auch die den Eingangsbereich des Berliner Funkhauses betreffenden Kameras (Nr. 3 und 4) sind nach Auffassung des Datenschutzbeauftragten nicht erforderlich, weil der Empfang den Bereich einsehen kann. Wenn die Videoüberwachung an dieser Stelle auch dem Fassadenschutz dient, könnte eine Aktivierung in den Abend- und Nachtstunden zulässig sein. Der Hans-Rosenthal-Platz müsste allerdings ausgespart bleiben.

Für eine Videoüberwachung der Parkplätze besteht nach Ansicht des Datenschutzbeauftragten keine Rechtfertigung, es sei denn, das Opferrisiko ist dort erhöht, was aber nur bei Dunkelheit der Fall sein dürfte.

Gegen die übrigen überwachten Bereiche hatte der Datenschutzbeauftragte keine Bedenken.

c) Dienstvereinbarung Videoüberwachung

Die schon im vorangegangenen Berichtszeitraum verhandelte Dienstvereinbarung zur Videoüberwachung ist bis zum Ablauf des hier relevanten Berichtszeitraums nicht geschlossen worden.

3. Aufzeichnung von Personal- und Redakteursversammlungen

Das Justizariat war gebeten, Leitlinien für die Aufzeichnung von Personal- und Redakteursversammlungen zu entwerfen. Anlass war die Veröffentlichung der Aufzeichnung einer Redakteursversammlung im Intranet. Es sind Fragen des Datenschutz- und des Arbeits- bzw. Personalvertretungsrechts betroffen.

Aus dem Datenschutzrecht, das beide Gremien bzw. deren Mitglieder bindet, sowie für den Personalrat aus dem Personalvertretungsrecht ergeben sich die folgenden Leitlinien, die der Datenschutzbeauftragte und das Justizariat der Geschäftsleitung sowie den genannten Gremien mitgeteilt und erläutert haben.

a) Personalversammlung

Eine Ton- und/oder Videoaufzeichnung sowie die Anfertigung von Wortprotokollen der Personalversammlung kann nur der Personalrat bzw. sein Vorsitzender als Veranstalter initiieren.

Die rechtliche Zulässigkeit der Aufzeichnung und/oder Wortprotokollierung hängt von der wirksamen Einwilligung aller von ihr Betroffenen ab. Betroffen sind bei einer Tonaufzeichnung und/oder Wortprotokollierung sämtliche Personen, die einen Wortbeitrag liefern, sowie solche natürlichen Personen, über die während der Versammlung identifizierbar gesprochen wird. Bei einer Videoaufzeichnung sind zudem auch alle übrigen Teilnehmer betroffen, wenn sie von der Kamera erfasst werden. Die Betroffenen müssen vor der Aufzeichnung (und vor der Erklärung ihrer Einwilligung) über den Zweck und die beabsichtigte Verwendung der Aufzeichnung aufgeklärt werden. Sie müssen in die Aufzeichnung vorher schriftlich einwilligen. Die Einwilligung kann – allerdings ohne Rückwirkung – widerrufen werden.

Die Verantwortung für die Einhaltung der vorstehenden (datenschutz-)rechtlichen Voraussetzungen trägt der Personalrat.

Die Veröffentlichung der Aufzeichnung oder des Wortprotokolls im Intranet ist wegen des strikten Gebots der Nichtöffentlichkeit der Personalversammlung grundsätzlich unzulässig.

b) Redakteursversammlung

Die rechtliche Zulässigkeit der Aufzeichnung und/oder Wortprotokollierung hängt von der wirksamen Einwilligung aller von ihr Betroffenen ab.

Betroffen sind bei einer Tonaufzeichnung und/oder Wortprotokollierung sämtliche Personen, die einen Wortbeitrag liefern, sowie solche natürlichen Personen, über die identifizierbar während der Versammlung gesprochen wird. Bei einer Videoaufzeichnung sind zudem auch alle übrigen Teilnehmer betroffen, soweit sie von der Kamera erfasst werden. Die Betroffenen müssen vor der Aufzeichnung (und vor der Erklärung ihrer Einwilligung) über den Zweck und die beabsichtigte Verwendung der Aufzeichnung aufgeklärt werden. Sie müssen in die Aufzeichnung vorher schriftlich einwilligen. Die Einwilligung kann – allerdings ohne Rückwirkung – widerrufen werden.

Die Verantwortung für die Einhaltung der vorstehenden (datenschutz-)rechtlichen Voraussetzungen trägt dasjenige Mitglied des Redakteursausschusses, das die Aufzeichnung veranlasst.

Die Veröffentlichung der Aufzeichnung und/oder Wortprotokollierung im Intranet oder sogar außerhalb des Hauses ist grundsätzlich zulässig. Die Veröffentlichung kann vom Deutschlandradio nicht ohne sachlichen Grund verweigert werden.

4. Automatische Aufzeichnung eingehender Anrufe

Bis zum Jahr 2002 wurden eingehende Anrufe im Funkhaus Köln bis zu einer Länge von zehn Minuten in einem überschreibbaren Speicher automatisch aufgezeichnet. Bewertete der angerufene Mitarbeiter den Anruf als Drohanruf o. ä., betätigte er einen Knopf und das gesamte Telefongespräch wurde von Beginn an auf Kassette überschrieben und dort weiter aufgezeichnet, bis der Mitarbeiter erneut besagten Knopf drückte. Der damalige Datenschutzbeauftragte empfahl, diese Praxis abzuändern. Daraufhin wurde die Höchstdauer auf vier Minuten reduziert.

Im Rahmen der Ausschreibung einer neuen Telefonanlage im Berichtszeitraum wurde der Datenschutzbeauftragte um seine Einschätzung gebeten. In einer ersten Stellungnahme hat er die Auffassung vertreten, dass eine Aufzeichnung bis zu einer Länge von zwei bis zweieinhalb Minuten ausreiche, um einen Drohanruf zu identifizieren und ggf. manuell dessen rückwirkende dauerhafte Speicherung auszulösen. Er hat ferner empfohlen, eine Technik anzuschaffen, die die flüchtige Aufzeichnung des Gesprächs mit oder kurz nach dessen Beendigung automatisch lösche.

Dem Datenschutzbeauftragten wurde indessen erläutert, dass es auf dem Markt eine Technik, die eine zeitlich beschränkte Aufzeichnung ermögliche, nicht gebe.

Obschon jeder eingehende Anruf also automatisch aufgezeichnet wird, hat der Datenschutzbeauftragte seine Zustimmung unter der Maßgabe des Folgenden erteilt: Wird während des Gesprächs der Auslöser zur Archivierung der Aufnahme nicht betätigt, ist die

Aufzeichnung mit Beendigung des Gesprächs nicht bzw. nur unter hohem Aufwand und mit Spezialkenntnissen abrufbar (erforderlich wären das Aufsuchen der Systemsteuerung und die Umgehung der räumlichen Sicherung des Rechners). De facto ist die Aufnahme, wenngleich physisch noch vorhanden, mit dem Gesprächsende gelöscht. Ferner wurde dem Datenschutzbeauftragten mitgeteilt, dass die Aufnahmevorrichtung nur an solchen Stellen installiert werde, an denen Anrufe im Haus typischerweise eingehen, also in der Telefonzentrale, beim Empfang, ggf. in der Intendanz und in den Schalträumen. In den allermeisten Fällen würden die Anrufer binnen weniger Sekunden durchgestellt, so dass ab diesem Zeitpunkt keine Aufzeichnung mehr erfolge. Es ist nicht zu erwarten, dass normale Anrufer länger als 2-2 1/2 Minuten - so die von dem Datenschutzbeauftragten als akzeptabel bezeichnete Zeitgrenze - in der Eingangsverbindung gehalten werden.

5. Speicherung von Hörertelefonnummern

Eine Redaktion des Funkhauses Berlin richtete an den Datenschutzbeauftragten die Frage, ob die Speicherung von Hörertelefonnummern zum Zwecke der Sicherstellung, dass nicht dieselben Hörer zu häufig in Sendungen mit Hörerbeteiligung erscheinen, zulässig ist. Der Datenschutzbeauftragte hat diese Frage bejaht. Er ist der Auffassung, dass diese Praxis vom sog. Medienprivileg des § 17 Deutschlandradio-Staatsvertrag (DRadio-StV) umfasst und damit ohne Einwilligung der Betroffenen zulässig ist. Er hat allerdings darauf hingewiesen, dass der Bestand an gespeicherten Telefonnummern regelmäßig überprüft und unverdächtige Nummern gelöscht werden müssen.

6. Einsatz von sog. Referrern

Ferner wurde der Datenschutzbeauftragte um seine Einschätzung gebeten, ob zur statistischen Auswertung des Nutzerverhaltens in dem Online-Auftritt des Deutschlandradios sog. Referrer eingesetzt werden dürfen, mit denen sich feststellen lässt, von welcher Internetseite der User zu dem Internet-Auftritt des Deutschlandradios gelangt ist.

Der Datenschutzbeauftragte hat gegen den Einsatz von Referrern keine Bedenken, wenn die gesetzlichen Bestimmungen des § 15 Abs. 3 TMG eingehalten werden. Er hat darauf hingewiesen, dass Änderungen der Datenschutzerklärung erforderlich sind.

E. Datenschutz bei der GEZ

Die GEZ ist eine Gemeinschaftseinrichtung der öffentlich-rechtlichen Rundfunkveranstalter der Bundesrepublik und besitzt keine eigene Rechtspersönlichkeit. Sie ist mit der Erhebung, Verarbeitung und Nutzung der Teilnehmerdaten von vielen Millionen Rundfunkteilnehmern beauftragt.

In Fragen des Datenschutzes beim Gebühreneinzug ist der jeweilige Rundfunkdatenschutzbeauftragte derjenigen Landesrundfunkanstalt zuständig, in deren Sendegebiet der betreffende Teilnehmer seinen Wohn- oder Geschäftssitz hat. In den Ländern Brandenburg, Berlin, Hessen und Bremen ist der jeweilige Landesdatenschutzbeauftragte zuständig. Deutschlandradio selbst betreibt - wie das ZDF - keinen Gebühreneinzug, diese Aufgabe nehmen die Landesrundfunkanstalten wahr. Insofern besteht keine Zuständigkeit

des Datenschutzbeauftragten des Deutschlandradios für den Umgang mit den Daten der Rundfunkteilnehmer.

Die betriebliche Datenschutzbeauftragte der GEZ ist Mitglied im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) und steht im ständigen Kontakt mit den Rundfunkdatenschutzbeauftragten. Die zahlreichen sich aus dem Gebühreneinzug ergebenden Fragen sind wesentlicher Teil der Beratungen innerhalb des AK DSB.

F. IVZ

Das Deutschlandradio ist beteiligt am Informationsverarbeitungszentrum (IVZ), das eine Gemeinschaftseinrichtung mehrerer Rundfunkanstalten ist. Beteiligt sind außerdem der NDR, MDR, Radio Bremen, SR und der rbb, bei dem das IVZ auch organisatorisch angesiedelt ist. Der Sitz des IVZ ist Potsdam. Das IVZ betreibt für Deutschlandradio nur verschiedene elektronische Archivsysteme, die sämtlich ausschließlich dem Programm dienen.

Für die datenschutzrechtliche Kontrolle sind die Datenschutzbeauftragten aller beteiligten Anstalten gemeinsam verantwortlich. Federführend ist die Datenschutzbeauftragte der Sitzanstalt, Frau Anke Naujock.

G. Informationsaustausch

I. KIT-Sitzungen

Im Berichtszeitraum hat der Datenschutzbeauftragte mehrfach an den Sitzungen der Koordinierungsgruppe innovative Techniken (KIT) teilgenommen. Dies ist ein internes Gremium, das durch die Rahmendienstvereinbarung zur Einführung innovativer Techniken errichtet wurde und der Abstimmung zwischen Geschäftsleitung und Personalrat bei Einführung oder Änderung von Datenverarbeitungssystemen dient. Die Treffen bieten auch für den Datenschutzbeauftragten, der ein Recht zur Teilnahme hat, die Möglichkeit, sich rechtzeitig über neu einzuführende Technologien zu informieren, die unter Umständen auch datenschutzrechtliche Bedeutung haben können. Es kann dadurch sichergestellt werden, dass frühzeitig datenschutzrechtliche Belange berücksichtigt werden können.

II. AK-DSB

Im Berichtszeitraum habe der Datenschutzbeauftragte regelmäßig an den Sitzungen des Arbeitskreises des Datenschutzbeauftragten der Rundfunkanstalten von ARD, ZDF und Deutschlandradio (AK-DSB) teilgenommen. Der Kreis ist ein Forum zum Austausch von Meinungen und Informationen über Vorgänge, die alle Rundfunkveranstalter betreffen oder die jedenfalls auch für andere Rundfunkanstalten von Interesse sind, weil sich dort vergleichbare Problemstellungen ergeben.

Köln, 27. Mai 2010

Dr. Markus Höppener