

Vorlage Nr. 28/2014 an den Rundfunkrat

TÄTIGKEITSBERICHT

des Datenschutzbeauftragten von Radio Bremen
Sven Carlson

für den Zeitraum vom

1. November 2014 bis zum 31. Oktober 2015

dem Rundfunkrat von Radio Bremen gemäß § 36 Satz 6
des Bremischen Datenschutzgesetzes in seiner Sitzung
am 10. Dezember 2015 vorgelegt.

Inhaltsverzeichnis:

A.	Vorbemerkung	- 4 -
B.	Stellung des Datenschutzbeauftragten von Radio Bremen	- 6 -
C.	Entwicklung des Datenschutzrechts	- 9 -
1.	Entwicklung des europäischen Datenschutzrechts	- 9 -
a.	EU-Datenschutz-Grundverordnung	- 9 -
b.	Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015 zum Safe-Harbor-Abkommen	- 10 -
2.	Entwicklung des Bundesrechts	- 12 -
a.	Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten	- 12 -
b.	Gesetz zur Erhöhung der Sicherheit informations- technischer Systeme (IT-Sicherheitsgesetz)	- 14 -
c.	Gesetzentwurf zur zivilrechtlichen Durchsetzung datenschutz-rechtlicher Vorschriften (Änderung UKlaG, UWG und BGB)	- 15 -
3.	Entwicklung des Landesrechts	- 16 -
	Evaluierung des Rundfunkbeitragsstaatsvertrag (RBStV)	- 16 -
D.	Datenschutz bei Radio Bremen	- 20 -
1.	Konzept für die dezentrale Verwaltung der Speicher- kapazitäten sowie der Ablage von Dateien	- 20 -
2.	Neues Antragsformular der Performa Nord GmbH	- 21 -

3.	Verhandlungen mit dem Personalrat über den Abschluss von verschiedenen Dienstvereinbarungen im IT- Bereich	- 22 -
4.	Online Bewerbungen bei Radio Bremen	- 22 -
5.	Datenschutz im journalistisch-redaktionellen Bereich	- 23 -
a.	Personalisierungskonzept für die ARD-Mediatheken	- 24 -
b.	Einsatz von sogenannten Drohnen im Rahmen der Berichterstattung	- 26 -
E.	Datenschutz beim Rundfunkbeitragseinzug	- 27 -
1.	Eingaben und Auskunftersuchen von Beitragszahlern und sonstigen Personen oder Stellen	- 28 -
2.	Überprüfung der Informationssicherheit bei der Creditreform Mainz Albert & Naujoks KG	- 30 -
3.	Klärungsschreiben des Beitragsservice an Flüchtlingsunterkünfte	- 30 -
F.	Datenschutz im Informationsverarbeitungszentrum (IVZ)	- 32 -
G.	Weitergehende Aktivitäten des Datenschutzbeauftragten	- 33 -
1.	Sitzungen des AK DSB	- 33 -
2.	Vertretung des AK DSB in der europäischen Datenschutzgruppe nach Art. 29 EU-Datenschutzrichtlinie	- 34 -
3.	Teilnahme an Fortbildungen und Veranstaltungen	- 34 -

A. Vorbemerkung

Wie bereits in meinem letzten Tätigkeitsbericht geschildert, werden die datenschutzrechtlichen Fragestellungen immer komplexer und vielschichtiger. Während es zu Beginn meiner Tätigkeit noch um z.B. die Zulässigkeit des Aushangs von Geburtstagslisten der Abteilungsmitarbeitenden in Sozialräumen ging, befasse ich mich derzeit in einem immer größeren Ausmaße mit Einschätzungen, die unseren Programmauftrag und den Bereich des Sendebetriebs betreffen.

Der Rundfunkbetrieb basiert in einem zunehmenden Maße auf IT-gestützten Systemen. Das gilt nicht nur für den Sendebetrieb, sondern auch für die übrige Betriebsorganisation. Viele Arbeitsprozesse werden elektronisch gesteuert, so dass der reibungslose Ablauf wesentlich von der eingesetzten Informationstechnik abhängt.

Darüber hinaus ist es für eine Rundfunkanstalt, die ihrem Programmauftrag zeitgemäß nachkommen will, unerlässlich, auch mittels mobiler Geräte auf dienstliche Daten zuzugreifen. Den Vorteilen einer möglichst effizienten, komfortablen sowie von Ort und Zeit unabhängigen Nutzung stehen aufgrund des zunehmenden Funktionsumfangs und des Vernetzungsgrades erhebliche Gefahren für die IT-Sicherheit gegenüber. Je sensibler dabei die verarbeiteten Daten sind, desto höher ist ihre Attraktivität für Angreifer.

Wie schwerwiegend die Folgen eines Hackerangriffs sein können, zeigt der im Mai 2015 bekannt gewordene Angriff auf das interne Netzwerk des Bundestages. Dabei sollen sich die Hacker Zugang zu den Administrator-Passwörtern verschafft haben, nachdem sie zunächst einen einzelnen Computer mit einem Trojaner infiziert hatten. Auch mehrere Wochen



nach der Entdeckung des Angriffs war die Spähsoftware noch auf den Rechnern aktiv.

Als Konsequenz daraus will der deutsche Bundestag seine IT-Sicherheit deutlich verbessern. So sollen beispielsweise die Mitarbeiterinnen und Mitarbeiter speziell geschult, das IT-Personal aufgestockt, die Erkennungssysteme für Schadsoftware verbessert und der Zugriff auf mehrere 10.000 Internetseiten blockiert werden. Zudem dürfen Abgeordnete zukünftig nur noch Passwörter mit mindestens acht Zeichen verwenden.

Dass auch Medien bevorzugte Ziele von Hackerangriffen sind, zeigt das Beispiel des französischen Fernsehsenders TV5 Monde, der im April 2015 gehackt wurde. Die Fernsehprogramme, die auch in Deutschland via Kabelnetz zu empfangen sind, waren stundenlang unterbrochen und auf den Onlineseiten und den Social-Media-Konten des Senders war Propaganda des sogenannten Islamischen Staates zu sehen.

Ein etwaiger Hackerangriff würde nicht nur den Schutz der personenbezogenen Daten, sondern auch die Sendefähigkeit gefährden. Das alles macht deutlich, dass der Schutz der IT-Infrastruktur eine immer größer werdende Herausforderung darstellt, die die einzelnen Mitarbeitenden einerseits und die Geschäftsführung andererseits anhaltend fordern wird.

Dass auch der Gesetzgeber hier Handlungsbedarf gesehen hat, zeigt das am 25. Juli 2015 in Kraft getretene Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). In diesem Zusammenhang verweise ich auf meine weitergehenden Ausführungen unter C. 2 b).



B. Stellung des Datenschutzbeauftragten von Radio Bremen

Die Rechtsgrundlagen für das Amt des Datenschutzbeauftragten von Radio Bremen haben sich im Berichtszeitraum nicht verändert.

Als Datenschutzbeauftragter von Radio Bremen bin ich gemäß § 36 Satz 2 des Bremischen Datenschutzgesetzes (BremDSG) in der Ausübung meines Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen unterstehe ich der Dienstaufsicht des Verwaltungsrates. Ich nehme diese Aufgabe neben meiner Tätigkeit als juristischer Mitarbeiter im Justizariat seit meiner Bestellung zum Datenschutzbeauftragten durch den Rundfunkrat am 19. Juni 2002 wahr.

Nach § 36 Satz 3 BremDSG habe ich die Einhaltung der Datenschutzvorschriften, soweit Radio Bremen personenbezogene Daten ausschließlich zu eigenen publizistischen Zwecken verarbeitet, zu überwachen. Ich habe die Aufgabe, den Einzelnen in seinem Grundrecht auf informationelle Selbstbestimmung zu schützen und dafür Sorge zu tragen, dass die geltenden datenschutzrechtlichen Bestimmungen durch und bei Radio Bremen beachtet und eingehalten werden.

Außerhalb dieser Zuständigkeit obliegt die Kontrolle der Einhaltung der Datenschutzbestimmungen bei Radio Bremen der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen. Eine entsprechende Aufteilung der Überwachungszuständigkeiten gilt ansonsten nur beim Rundfunk Berlin-Brandenburg und beim Hessischen Rundfunk.

Die Kontrollkompetenz der Landesdatenschutzbeauftragten beschränkt sich in der Praxis auf den Bereich des Rundfunkteilnehmerdaten-



schutzes. Die sich daraus ergebende Zusammenarbeit war jederzeit konstruktiv und kollegial.

Jenseits dieser positiven Erfahrungen halte ich die in Bremen geltende gespaltene Kontrollzuständigkeit für den Bereich der Datenverarbeitung bei Radio Bremen nach wie vor für verfassungsrechtlich bedenklich.

Gemäß § 36 Satz 6 BremDSG habe ich als Datenschutzbeauftragter dem Rundfunkrat jährlich einen Bericht über meine Tätigkeit zu erstatten. Mit diesem Tätigkeitsbericht wird die Entwicklung des Datenschutzes bei Radio Bremen für die Zeit vom 1. November 2014 bis zum 31. Oktober 2015 dokumentiert. Der Tätigkeitsbericht umfasst sowohl meine Aktivitäten als Datenschutzbeauftragter für den journalistisch-redaktionellen Bereich als auch meine Betätigung als sogenannter behördlicher Datenschutzbeauftragter.

Förmliche Beanstandungen mussten im Berichtszeitraum nicht ausgesprochen werden. Die Themen Datenschutz und Datensicherheit nehmen im Bewusstsein aller Mitarbeiterinnen und Mitarbeiter - auch dank des Engagements des Personalrats - eine nach wie vor wichtige Rolle ein. Ich werde in aller Regel schon präventiv in die jeweiligen Prozesse eingebunden und um datenschutzrechtliche Einschätzungen gebeten. Das erleichtert nicht nur meine Arbeit, sondern sorgt auch dafür, dass die datenschutzrechtlichen Anforderungen von Beginn an berücksichtigt werden.

Dank gebührt in diesem Zusammenhang insbesondere André Busjaeger, der die Abteilung „Koordination Technik“ leitet, sowie Malte Spiegelberg, dem Datenschutzbeauftragten der Bremedia Produktion GmbH. Beide standen mir bei technischen Fragestellungen stets kompetent mit Rat und Tat zur Seite.



Dieser Tätigkeitsbericht wird, nachdem er dem Rundfunkrat zur Kenntnisnahme vorgelegt worden ist, im Online-Angebot von Radio Bremen veröffentlicht werden. Er wird unter

<http://www.radiobremen.de/unternehmen/organisation/datenschutz100.html>

abrufbar sein.

C. Entwicklung des Datenschutzrechts

Im Nachfolgenden soll ein kurzer Überblick über die Entwicklungen im Datenschutzrecht auf europäischer und nationaler Ebene gegeben werden, die auch meine Tätigkeit als Datenschutzbeauftragter von Radio Bremen betreffen bzw. betreffen können.

1. Entwicklung des europäischen Datenschutzrechts

a. EU-Datenschutz-Grundverordnung

Wie bereits in meinem letzten Tätigkeitsbericht ausgeführt, versuchen die Europäische Kommission, das Europäische Parlament sowie der Rat der Europäischen Union im sogenannten Trilog eine gemeinsame Position zur EU-Datenschutz-Grundverordnung zu finden. Die entsprechenden Verhandlungen dauern seit dem Sommer an und sollen sich zum Teil schwierig gestalten. Ob das gemeinsam erklärte Ziel, die Verhandlungen Ende 2015 abzuschließen, erreicht werden kann, bleibt abzuwarten.

Die EU-Datenschutz-Grundverordnung wird dann die technisch überholte EG-Datenschutzrichtlinie von 1995 ersetzen. Im Gegensatz zur noch gültigen Richtlinie, die von den EU-Mitgliedsstaaten in nationales Recht umgesetzt werden musste, wird die EU-Datenschutz-Grundverordnung ohne Umsetzungsakt unmittelbar in allen EU-Mitgliedsstaaten Geltung erlangen. Den Mitgliedsstaaten wird es daher nicht möglich sein, den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken.

Ziel der EU-Datenschutz-Grundverordnung ist es, einerseits die Regelungen für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit zu vereinheitlichen und

andererseits den freien Datenverkehr innerhalb des europäischen Binnenmarktes zu garantieren.

Die Interessen des öffentlich-rechtlichen Rundfunks sind in der Entwurfsfassung des Art. 80 berücksichtigt worden. Danach können Mitgliedstaaten „für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen oder Ausnahmen vorsehen“. Damit ist den Landesgesetzgebern die Aufgabe zugewiesen, entsprechende Bestimmungen zu schaffen.

b. Urteil des Europäische Gerichtshofs vom 6. Oktober 2015 zum Safe-Harbor-Abkommen

Der Europäische Gerichtshof (EuGH) hat am 6. Oktober 2015 das Safe-Harbor-Abkommen zwischen den USA und der EU für ungültig erklärt, da es in seiner aktuellen Form nicht mit dem europäischen Recht zu vereinbaren sei.

Dieses Abkommen erlaubte es Konzernen wie z.B. Facebook oder Amazon bislang, die Daten ihrer europäischen Kundinnen und Kunden auf Servern in den USA zu verarbeiten, ohne zuvor gesondert geprüft zu haben, ob das den europäischen Datenschutzbestimmungen entspricht. Nach Auffassung des EuGH sind die Daten europäischer Nutzerinnen und Nutzer in den USA nicht ausreichend vor dem Zugriff von Behörden geschützt.

Dieser Entscheidung lag der seit Jahren andauernde Rechtsstreit zwischen einem klagenden Datenschutzaktivisten aus Österreich und der irischen Datenschutzbehörde zu Grunde. Der Kläger hatte den mangelnden Datenschutz bei Facebook kritisiert, für den Irland zuständig ist, weil das US-Unternehmen dort seinen Europasitz hat. Irlands Datenschutz-

beauftragter sah die Datenverarbeitung durch Facebook als zulässig an, da man sich dabei auf das Safe-Harbor-Abkommen stützen könne.

Daraufhin strengte der Kläger eine Klage vor dem obersten irischen Gerichtshof, dem Supreme Court, an, der den Fall dem EuGH vorlegte. Dieser führte in seiner Urteilsbegründung aus, dass die EU-Kommission dem Safe-Harbor-Abkommen hätte nicht zustimmen dürfen, da die US-Behörden nie an die entsprechenden Datenschutzbestimmungen gebunden gewesen wären.

Durch die EuGH-Entscheidung ist es nun erforderlich, den Austausch von Daten zwischen Unternehmen in den USA und der Europäischen Union neu zu regeln.

Es ist davon auszugehen, dass dieses Urteil keine Relevanz für Radio Bremen haben dürfte - abgesehen von Beschwerden und Anfragen. Wir speichern mittels unserer DV-Anwendungen oder Onlineangebote keine personenbezogenen Daten in den USA. Die journalistischen Inhalte, die wir auf Facebook verbreiten, sind allesamt solche, die vorab bereits ausgestrahlt und somit schon einer breiten Öffentlichkeit zugänglich gemacht worden sind.

2. Entwicklung des Bundesrechts

a. Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Der deutsche Bundestag hat am 16. Oktober 2015 das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ verabschiedet.

Danach müssen Telekommunikationsunternehmen Internet- und Verkehrsdaten jedes Bürgers anlasslos für zehn Wochen speichern. Das umfasst solche technischen Informationen, die bei der Nutzung eines Telekommunikationsdienstes (Telefonie, Internetnutzung) beim jeweiligen Telekommunikationsunternehmen (Provider) anfallen. Daneben sind Standortdaten vier Wochen zu speichern. Die entsprechenden Nutzungsinhalte müssen dagegen nicht dokumentiert werden.

Dies ist ein weiterer Versuch, ein Gesetz zu schaffen, das die anlasslose Speicherung von Daten einer Vielzahl von Menschen von und für öffentliche Stellen zum Gegenstand hat. Das erste entsprechende gesetzgebende Unterfangen hatte das Bundesverfassungsgericht (BVerfG) in seiner Entscheidung vom 2. März 2010 gestoppt und das im Jahr 2007 in Kraft getretene Gesetz zur Vorratsdatenspeicherung für verfassungswidrig erklärt. Zur Begründung hatte das Gericht ausgeführt, dass das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe und zudem die Hürden für staatliche Zugriffe auf die Daten zu niedrig seien. Eine Vorratsdatenspeicherung verstößt allerdings auch nach Ansicht des BVerfG nicht generell gegen das Grundgesetz.

Das damalige Gesetz zur Vorratsdatenspeicherung basierte auf einer entsprechenden EU-Richtlinie, die - wie in meinem letzten Tätigkeitsbericht berichtet - am 8. April 2014 vom EuGH für ungültig erklärt worden war. Nach Auffassung der erkennenden Richterinnen und Richter beinhaltet die Regelung „einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der sich nicht auf das absolut Notwendige beschränkt“.

Mit dem Wegfall der europarechtlichen Grundlage war auch die Bundesregierung zunächst von ihrem Vorhaben abgerückt, schnell ein neues Gesetz zur Vorratsdatenspeicherung zu erlassen. Auch wenn es zunächst so aussah, als würden sich die Koalitionspartner von CDU/CSU und SPD nicht verständigen können, haben sie nunmehr das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vorgelegt.

In einer gemeinsamen Stellungnahme haben ARD, ZDF, der Bundesverband Deutscher Zeitungsverleger (BDZ), der Deutsche Journalisten Verband (DJV), der Deutsche Presserat, der Verband Deutscher Zeitschriftenverleger (VDZ), die Vereinte Dienstleistungsgewerkschaft (dju in ver.di) und der Verband Privater Rundfunk und Telemedien (VPRT) das Gesetzesvorhaben kritisiert, weil es die Pressefreiheit gefährde. Die vorgesehene Speicherung von Telefonnummern, IP-Adressen und Standortdaten untergrabe den Schutz der Informanten, zu dem insbesondere Journalistinnen und Journalisten berechtigt und ethisch verpflichtet sind. Zudem fehle es an einem Schutz von Berufsgeheimnisträgern vor der Speicherung ihrer elektronischen beruflichen Kontakte.

Genau dies hatte der EuGH in seiner oben genannten Entscheidung vom 8. April 2014 allerdings beanstandet, da es der nunmehr für ungültig erklärten EU-Richtlinie an eben solchen Regelungen fehlte.

Ob das geschaffene Gesetz die verfolgte Zielsetzung der effektiven Bekämpfung der Kriminalität und des Terrorismus tatsächlich fördert, ist nach wie vor fraglich. Statistiken belegen dies jedenfalls bis heute nicht.

Auch im Übrigen ist zweifelhaft, ob das Gesetz den Anforderungen der Rechtsprechung des EuGH und des BVerfG genügt. Nachdem die Gegner des Gesetzes unmittelbar nach seinem Inkrafttreten rechtliche Schritte angekündigt hatten, haben einige Bundestagsabgeordnete sowie Journalisten- und Medienverbände beim BVerfG eine einstweilige Anordnung beantragt. Sie wollen erreichen, dass die Speicherpflicht der Telekommunikationsanbieter bis zur Entscheidung über eine Verfassungsbeschwerde ausgesetzt wird.

b. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist am 25. Juli 2015 in Kraft getreten.

Trotz des Bestehens eines auf Freiwilligkeit beruhenden Verfahrens zur Meldung von IT-Sicherheitsvorfällen der Wirtschaft hat sich der Gesetzgeber entschieden, die Anforderungen an die IT-Sicherheit für bestimmte Bereiche zu normieren. Mit dem IT-Sicherheitsgesetz sollen die Betreiber besonders gefährdeter Infrastrukturen verpflichtet werden, ihre Datenetze besser vor Hacker-Angriffen zu schützen.

Nach dem IT-Sicherheitsgesetz erfassen die gefährdeten Infrastrukturen die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen und solche Einrichtungen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die abschließende Festlegung dieser gefährdeten Infrastrukturen soll einer noch zu erlassenden Rechtsverordnung vorbehalten bleiben.

Auch wenn die Rundfunkanstalten eine hohe Bedeutung für das Funktionieren des Gemeinwesens haben, fallen Sie nicht in den Anwendungsbereich des IT-Sicherheitsgesetzes, weil es dem Bund an einer entsprechenden Gesetzgebungskompetenz mangelt. Insoweit bleibt abzuwarten, wie die Bundesländer hier vorgehen. Es erscheint jedenfalls nicht unwahrscheinlich, dass auch entsprechende landesgesetzliche Bestimmungen erlassen werden.

Das IT-Sicherheitsgesetz schreibt neben der obligatorischen Meldung von IT-Sicherheitsvorfällen auch Mindeststandards für die IT-Sicherheit bei den Betreibern gefährdeter Infrastrukturen vor. Dazu sollen die jeweiligen Branchen selbst Standards entwickeln, die dann vom Bundesamt für Sicherheit in der Informationstechnik (BSI) genehmigt werden. Zudem sollen die Unternehmen alle zwei Jahre nachweisen, dass sie die Anforderungen noch erfüllen.

c. Gesetzentwurf zur zivilrechtlichen Durchsetzung datenschutzrechtlicher Vorschriften (Änderung UKlaG, UWG und BGB)

Im Februar 2015 hat die Bundesregierung den Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucher-

schützenden Vorschriften des Datenschutzrechts vorgelegt. Dieses sieht explizit ein Verbandsklagerecht bei Datenschutzverstößen vor und soll den Verbraucherschutzverbänden die Verfolgung von Datenschutzverstößen ermöglichen. Das Gesetz befindet sich derzeit in der parlamentarischen Beratung.

Die Datenschutzbeauftragten sehen diese Entwicklung nicht unkritisch. Der Datenschutz wird danach stärker als bislang dem Einfluss von Entscheidungen der Zivilgerichte ausgesetzt. Hierdurch ist eine gewisse Konkurrenz zur Tätigkeit der datenschutzrechtlichen Aufsichtsbehörden zu erwarten. Es besteht die Sorge, dass die Zivilgerichte bei ihrer einzel-fallbezogenen und durch den Klageanspruch limitierten Tätigkeit nicht unbedingt die datenschutzrechtlichen Gegebenheiten in umfassender und korrekter Weise abbilden können.

3. Entwicklung des Landesrechts

Evaluierung des Rundfunkbeitragsstaatsvertrag (RBStV)

Wie bereits in meinem letzten Tätigkeitsbericht erläutert, war eine umfassende Evaluierung des Rundfunkbeitragsstaatsvertrages (RBStV) im Zeitraum von zwei Jahren nach seinem Inkrafttreten vorgesehen. Dabei sollen die Auswirkungen auf den privaten, gewerblichen und öffentlichen Bereich beleuchtet werden.

Aus datenschutzrechtlicher Sicht lässt sich festhalten, dass mit Inkrafttreten des RBStV die Erforschung von Lebenssachverhalten in Familien und Wohngemeinschaften hinfällig geworden ist, da es nicht mehr erforderlich ist festzustellen, wie viele Geräte zum Rundfunkempfang in einer Wohnung bereitgehalten werden. Dies hat dazu geführt, dass die Rund-

funkanstalten darauf verzichten, Beauftragte zur Feststellung der Rundfunkbeitragspflicht einzusetzen.

Zudem übermitteln die Einwohnermeldeämter dem Beitragsservice von ARD, ZDF und Deutschlandradio (Beitragsservice) seit März 2013 Angaben zu Namen, Adresse, Doktorgrad, Familienstand, Geburtsdatum und Einzugsdatum aller in Deutschland gemeldeten Bürgerinnen und Bürger. Mittels dieses einmaligen Meldedatenabgleichs nach § 14 Absatz 9 RBStV soll sichergestellt werden, dass alle beitragspflichtigen Bürgerinnen und Bürger beim Beitragsservice gemeldet sind, um ihrer Pflicht zur Zahlung des Rundfunkbeitrags nachzukommen.

Die Schreiben, die die Rundfunkanstalten wegen des einmaligen Meldedatenabgleichs von Bürgerinnen und Bürgern erhalten haben, sind weniger als Beschwerden denn als Ersuchen zu werten, mit denen weitergehende Informationen zu diesem Thema erbeten werden. In der Vielzahl der Fälle reichte für die Erledigung ein Hinweis auf die gesetzgeberische Absicht, eine höhere Gerechtigkeit beim Einzug des Rundfunkbeitrags zu erreichen, aus.

Aus Sicht der Rundfunkanstalten muss einer Erosion des Rundfunkteilnehmerbestandes dadurch vorgebeugt werden, dass auch zukünftig regelmäßig ein Meldedatenabgleich erfolgen kann. Dies ist erforderlich, um einen aktuellen und korrekten Datenbestand vorhalten zu können. Dafür reicht die bestehende Meldedatenübermittlungsverordnung nicht aus, da über diesen Weg nur Daten von volljährigen Personen mitgeteilt werden, die sich beim jeweiligen Meldeamt an- oder abgemeldet haben bzw. verstorben sind. Trotz der gesetzlichen Anzeigepflicht des in der Wohnung verbleibenden Gesamtschuldners erhalten die Rundfunkanstalten bzw. der Zentrale Beitragsservice in vielen Fällen keine Information darüber, wer für die entsprechende Wohnung als neuer Beitragspflichtiger ange-



schrieben werden kann. Ebenso würde das „Hineinwachsen“ von Jugendlichen in die Beitragspflicht vielfach vollständig unentdeckt bleiben.

Die zu erwartende Erosion des Datenbestandes lässt sich anhand statistischer Größen ohne weiteres nachvollziehen: Im Durchschnitt sind in den vergangenen fünf Jahren etwa 400.000 Menschen jährlich gestorben und finden pro Jahr ca. 800.000 Umzüge wegen Scheidung oder Trennung statt. Die Anzahl der Jugendlichen, die schon in einer eigenen Wohnung leben, wenn sie das 18. Lebensjahr vollenden, ist unbekannt.

Die Datenschützer von ARD, ZDF und Deutschlandradio (AK DSB) halten eine regelmäßige Wiederholung des vollständigen Meldeabgleichs in einem Abstand von fünf bis sechs Jahren für geboten, da kein ebenso geeignetes und milderer Mittel zur Erreichung der Ziele zur Verfügung steht. Die Anmietung von Adressen bei kommerziellen Adresshändlern stellt ebenso wie der Einsatz von Beauftragten zur Feststellung der Beitragspflicht keine Alternative dar. Die Qualität der Daten, die der Beitragsservice über Adresshändler oder Beauftragte erhalten hat, entspricht bei weitem nicht der Qualität der Daten, die er durch die Meldeämter erhält. Zudem dürften die Beeinträchtigungen der Beitragspflichtigen, die mit einer etwaigen Überprüfung vor Ort durch den Beauftragten einhergehen, nicht unerheblich sein.

Darüber hinaus hat der AK DSB weitere Änderungen des RBStV angeregt. Beispielsweise sollte eine Rechtsgrundlage für die Erhebung und Nutzung von Telefonnummern und E-Mail-Adressen aus öffentlich zugänglichen Quellen im nicht-privaten Bereich geschaffen werden, da auf diese Weise auch dort die Beeinträchtigungen vor Ort eingeschränkt werden können. Bislang kann die Beitragspflicht oftmals nur durch Recherchen am Geschäftssitz festgestellt werden. Außerdem hat der AK DSB vorgeschlagen, den Kreis der zur Auskunft Verpflichteten nach § 9

radiobremen 

Absatz 1 RBStV ersatzlos zu streichen. Dort ist neben dem Eigentümer "der vergleichbar dinglich Berechtigte" aufgeführt. Dieser Begriff erscheint nicht ausreichend bestimmt, weil es dafür weder eine gesetzliche Definition noch einen beispielsweise durch die Rechtsprechung geprägten feststehenden Kreis von Personen gibt.

D. Datenschutz bei Radio Bremen

Die datenschutzrechtlichen Aktivitäten bei Radio Bremen waren im Berichtszeitraum von zahlreichen internen Anfragen von Führungskräften, Projektverantwortlichen und anderen Mitarbeiterinnen und Mitarbeitern zu unterschiedlichen Themen geprägt. Dabei ging es regelmäßig um Beratungen im Hinblick auf datenschutzrechtlich relevante Sachverhalte sowie um damit im Zusammenhang stehende Auslegungsfragen.

Neben der allgemeinen Beratung bei Einzelfragen wird auch darauf geachtet, dass die gesetzlichen Regelungen zum Datenschutz und zur Datensicherheit Eingang in etwaige Verträge finden, die zwischen Radio Bremen und Auftragnehmern geschlossen werden. Insbesondere im IT-Bereich, in dem Auftragnehmer im Rahmen ihrer Tätigkeit für Radio Bremen regelmäßig auch mit personenbezogenen Daten in Berührung kommen, wurde mittels entsprechender Regelungen in den zu Grunde liegenden Verträgen sichergestellt, dass die datenschutzrechtlichen Anforderungen beachtet und eingehalten werden.

1. Konzept für die dezentrale Verwaltung der Speicherkapazitäten sowie der Ablage von Dateien

Es ist beabsichtigt, die Verwaltung der vorhandenen Speicherkapazitäten und der Ablage von Dateien zukünftig dezentral zu organisieren. Dafür sollen Ordnerverantwortliche ernannt werden, die für die Verwaltung der gemeinsamen Dateien und Ordnern ihrer Redaktion bzw. Abteilung zuständig sein werden. Die Rechte der Administratoren bleiben davon unberührt.

Ziel ist es, die Dateien und Ordner am Arbeitsplatz sinnvoll und orientiert an den jeweiligen Bedürfnissen zu organisieren. Den Redaktionen und Abteilungen wird es dadurch möglich sein, effizient und ohne Zeitverlust den eigenen Anforderungen besser gerecht zu werden. Außerdem dürfte die dezentrale Speicherverwaltung helfen, die bestehenden Ressourcen sinnvoll zu nutzen.

Die Berechtigungen beinhalten keine Leserechte bzw. Rechte zur Löschung, sondern beschränken sich auf die Einrichtung von Zugriffsrechten innerhalb der Redaktion bzw. Abteilung. Alle Zugriffsveränderungen werden protokolliert.

Die Ernennung der Ordnerverantwortlichen erfolgt in Absprache mit der jeweiligen Redaktions- bzw. Abteilungsleitung. Eine Weitergabe seiner Zugriffsrechte ist dem Ordnerverwalter nicht möglich.

Im Rahmen meiner Befassung konnte auch den datenschutzrechtlichen Anforderungen Genüge getan werden, so dass der Einführung des Konzepts insoweit nichts im Wege steht.

2. Neues Antragsformular der Performa Nord GmbH

Radio Bremen hat die Performa Nord GmbH in den Jahren 2003 und 2004 damit beauftragt, die hiesigen Anträge auf Gewährung von Beihilfe und Familienzuschlag zu bearbeiten und zu bescheiden.

Im Zuge der Überarbeitung der in diesem Zusammenhang genutzten Formulare wurden auch Änderungen vorgenommen, die aus datenschutzrechtlichen Gründen nicht zulässig waren. So war es nicht erforderlich ein Feld vorzusehen, um die Daten der Bankverbindung anzugeben, da die jeweiligen Beiträge zwar von der Performa Nord GmbH er-



rechnet, aber nicht gezahlt werden. Dies erfolgt weiterhin durch Radio Bremen.

3. Verhandlungen mit dem Personalrat über den Abschluss von verschiedenen Dienstvereinbarungen im IT- Bereich

Die Verhandlungen mit dem Personalrat über den Abschluss diverser Dienstvereinbarungen im IT-Bereich sind abgeschlossen. Nunmehr bedarf es noch der formalen Verabschiedung durch das Direktorium und den Personalrat. Wegen weiterer Einzelheiten verweise ich auf die Tätigkeitsberichte der vergangenen Jahre.

4. Online-Bewerbungen bei Radio Bremen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen hat die bei Radio Bremen bestehende Praxis, dass an einem Betriebspraktikum interessierte Bewerberinnen und Bewerber sich ausschließlich online bewerben konnten, obgleich keine sichere Übertragung der teilweise sensiblen Daten gewährleistet war, kritisiert.

Daraufhin teilte die Personalleitung von Radio Bremen ihr mit, dass sie den Ausschreibungstext für Betriebspraktika so geändert habe, dass nunmehr Bewerbungen zusätzlich auch auf dem Postweg möglich seien.

Erst durch die Befassung der Landesbeauftragten für Datenschutz und Informationsfreiheit habe ich von diesem Verfahren Kenntnis erlangt. Seitens der Personalabteilung wollte man durch die Schaffung der Online-Bewerbung sicherstellen, dass den in der Regel jungen Bewerberinnen und Bewerbern ein zeitgemäßer Weg zur Verfügung gestellt wird, um die erforderlichen Unterlagen an Radio Bremen schicken zu können.



Nunmehr haben sie alternativ wieder die Möglichkeit, den postalischen Versand zu wählen.

Unter dem Gesichtspunkt, dass die Datenübertragung via Internet ohne geeignete Verschlüsselungsmaßnahmen nicht geschützt ist und mit entsprechenden Wissen weltweit eingesehen und ausgewertet werden kann, ohne dass die Betroffenen davon Kenntnis erlangen, sollten technische Sicherheitsvorkehrungen geschaffen werden, die es den Bewerberinnen und Bewerber ermöglichen, ihre Online-Bewerbung ausreichend gesichert an Radio Bremen zu senden.

5. Datenschutz im journalistisch-redaktionellen Bereich

Im Bereich der Datenverarbeitung zu journalistisch-redaktionellen Zwecken haben mich das Personalisierungskonzept für die Mediatheken der ARD sowie der Einsatz von sogenannten Drohnen im Rahmen der Berichterstattung beschäftigt.

Im Übrigen waren im journalistisch-redaktionellen Bereich keine gesonderten Kontrollmaßnahmen erforderlich, da die datenschutzrechtlichen Vorgaben weitestgehend von den Regelungen des Presserechts (z.B. Gegendarstellung, Richtigstellung, Unterlassung, Widerruf) und des Radio Bremen-Gesetzes (Eingaben und Programmbeschwerden) abgedeckt sind.

Da die Beantwortung derartiger Fragestellungen in den Tätigkeitsbereich des Justiziariats fällt, ist sichergestellt, dass ich als Datenschutzbeauftragter davon Kenntnis erlange, zumal ich derartige Angelegenheiten in der Regel auch selbst bearbeite.

a. Personalisierungskonzept für die ARD-Mediatheken

Allen interessierten Nutzerinnen und Nutzern soll es ermöglicht werden, aus dem gesamten Angebot der ARD-Mediatheken individuell auf Videos und Audiobeiträge zuzugreifen. Dafür sollen Funktionen geschaffen werden, die die Nutzerinnen und Nutzer in die Lage versetzen, zielgerichtet und schnell auf Angebote zuzugreifen, die ihren Interessen entsprechen. Hier wird beispielsweise an Favoriten-, Merk- und Playlisten, Empfehlungen, Push-Nachrichten, Social-Media-Einbindungen gedacht.

Die Personalisierungsfunktionen sollen dabei dem ausschließlichen Zweck dienen, ein konsistentes und nutzungsfreundliches Angebot über alle Plattformen hinweg zu schaffen. Die Daten werden nicht zu kommerziellen Zwecken genutzt werden, selbstverständlich ist der Handel mit Daten ausgeschlossen. Sofern für spezielle Projekte externe Dienstleister einbezogen oder beauftragt werden, werden diese ihrerseits zur Einhaltung der datenschutzrechtlichen Bestimmungen und Vorgaben verpflichtet. Gleichzeitig wird eine zufriedenstellende Nutzung der Inhalte auch ohne eine Registrierung und Personalisierung sichergestellt sein.

Den Nutzerinnen und Nutzern wird es jederzeit frei stehen, sich von Personalisierungsfunktionen und optionalen Nutzungsmessungen abzumelden. Eine sinnvolle Nutzung der Angebote ist dennoch gewährleistet. Diese Grundsätze werden für die Nutzerinnen und Nutzer transparent dargestellt und sind jederzeit einsehbar. Es entstehen dem Nutzer keine zusätzlichen Kosten.

Soweit Inhalte unter Einbeziehung von Drittplattformen verbreitet werden, wird den Nutzerinnen und Nutzern im Rahmen der gegebenen Möglichkeiten ebenfalls offen und transparent aufgezeigt, welche daten-



schutzrelevanten Geschäftsbedingungen für die Nutzung der jeweiligen Drittplattformen gelten.

Für die Nutzung der Angebote ist die Verwendung eines Klarnamens nicht erforderlich. Es ist ausreichend, wenn die Registrierung mittels eines Pseudonyms erfolgt. Damit wird den Vorgaben des Telemediengesetzes genügt.

Auf die Daten der Nutzerinnen und Nutzer soll nur insoweit zugegriffen werden, als dies für die spezifischen Angebote notwendig, redaktionell intendiert und vom Nutzer gewollt ist. Weil Technologien, Darstellungsformen von Inhalten und ihre Plattformen zur Verbreitung einem ständigen Wandel unterliegen, wird das Personalisierungskonzept regelmäßig anhand der datenschutzrechtlichen Anforderungen aktualisiert und weiterentwickelt.

Der Entwurf eines entsprechenden Personalisierungskonzeptes ist dem AK DSB zur Prüfung vorgelegt worden und hat grundsätzliche Zustimmung gefunden. Die entsprechenden Änderungs- und Ergänzungsvorschläge müssen noch eingearbeitet werden.

b. Einsatz von sogenannten Drohnen im Rahmen der Berichterstattung

In meiner programmrechtlichen Zuständigkeit hatte ich mich mit dem Einsatz von Drohnen im Rahmen der Berichterstattung zu beschäftigen.

Im Gegensatz zur Beschaffung von Bildern, die mittels auf Kränen installierten oder von Hubschraubern aus bedienten Kameras entstehen, können auf Drohnen angebrachte Kameras schnell und kostengünstig zum Einsatz gebracht werden.

Dabei nutzt Radio Bremen keine eigenen oder von Beschäftigten privat erworbenen Geräte, sondern beauftragt schon aus Gründen der Haftung gewerbliche Anbieter mit der Anfertigung solcher Ausnahmen.

Da die Aufnahmen mittels Drohnen im Rahmen der Berichterstattung dem Medienprivileg unterfallen, gelten die datenschutzrechtlichen Bestimmungen nicht. Mit dem Programmbereich bin ich so verblieben, dass dort, wo Rechte Dritter (insbesondere das Recht am eigenen Bild) durch die Aufnahmen verletzt werden könnten, ein Einsatz von Drohnen nur dann erfolgen kann, wenn dies vorab mit dem Justizariat abgestimmt worden ist.

E. Datenschutz beim Rundfunkbeitragseinzug

Der im Juli 2015 veröffentlichte Geschäftsbericht des Beitragsservice für das Jahr 2014 weist 44,54 Millionen Beitragskonten aus. Im Bestand finden sich annähernd 39,3 Millionen Wohnungen, rund 3,4 Millionen Betriebsstätten, ca. eine Million Gästezimmer und Ferienwohnungen sowie nahezu 4,2 Millionen Kraftfahrzeuge.

Für Bremen und Bremerhaven sind insgesamt 377.828 Beitragskonten angemeldet. Geführt werden 335.107 Wohnungen, 31.783 Kraftfahrzeuge, 24.674 Betriebsstätten sowie 7.193 Gästezimmer und Ferienwohnungen.

Im Jahre 2014 übermittelten die Meldebehörden dem Beitragsservice 45,8 Millionen Datensätze. Von den insgesamt 3,2 Millionen Personen, die um Klärung von Beitragssachverhalten gebeten wurden, haben rund 1,7 Millionen Personen Beitragskonten angemeldet. Darüber hinaus führten die Daten aus der einmaligen Meldedatenübermittlung in rund 3,4 Millionen Fällen zu einer Aktualisierung der Beitragskonten und trugen somit dazu bei, dass die Beiträge der zuständigen Landesrundfunkanstalt zugeordnet werden konnten.

Für die Datenschutzkontrolle beim Beitragseinzug ist der jeweilige Datenschutzbeauftragte der einzelnen Landesrundfunkanstalten bezogen auf die Rundfunkteilnehmerinnen und -teilnehmer des entsprechenden Sendegebietes zuständig. Dabei sind die landesspezifischen Regelungen für den Datenschutz zu beachten. In den Ländern Berlin, Brandenburg (Rundfunk Berlin-Brandenburg), Bremen (Radio Bremen) und Hessen (Hessischer Rundfunk) üben die Landesdatenschutzbeauftragten die Kontrollfunktion für die nicht-journalistischen Daten der jeweiligen Landesrundfunkanstalten aus (vgl. unter B.).



Unterstützt werden alle Rundfunkdatenschutzbeauftragten bzw. die genannten Landesdatenschutzbeauftragten gemäß § 11 Abs. 2 RBStV durch die vor Ort tätige interne Datenschutzbeauftragte des Beitragsservice. Da sie Mitglied des AK DSB ist, ist ein intensiver Austausch zwischen den Landesrundfunkanstalten und dem Beitragsservice in diesem Bereich auch strukturell sichergestellt. Die Zusammenarbeit mit der Datenschutzbeauftragten des Beitragsservice war jederzeit problemlos und konstruktiv.

1. Eingaben und Auskunftersuchen von Beitragszahlern und sonstigen Personen oder Stellen

Grundsätzlich werden - sofern keine Besonderheiten ersichtlich sind - die Eingaben und Auskunftersuchen der im Sendegebiet von Radio Bremen ansässigen Petenten von der Stelle beantwortet, an die die Anfrage gerichtet ist. Vornehmlich sind dies der Beitragsservice und die Rundfunkbeitragsabteilung des Norddeutschen Rundfunks, der seit 2001 alle mit dem Rundfunkgebühreneinzug bei Radio Bremen im Zusammenhang stehenden Tätigkeiten übernommen hat.

Im Berichtszeitraum wurden beim Beitragsservice drei Anfragen, beim Norddeutschen Rundfunk vier Anfragen und beim Datenschutzbeauftragten von Radio Bremen fünf Anfragen von betroffenen Beitragszahlern gestellt. In den meisten Fällen beehrten die Anfragenden Auskünfte über die zu ihrer Person gespeicherten Daten bzw. zur Herkunft dieser Daten. Zudem ging es in einigen Anfragen um die Zulässigkeit des einmaligen Meldedatenabgleichs.



Hervorzuheben ist dabei die nachfolgende Eingabe:

Ein Beitragszahler kritisierte, dass der Beitragsservice Briefumschläge mit Sichtfenstern verwende und im dortigen Adressfeld auch die Beitragsnummer ersichtlich sei. So würden alle übrigen Bewohnerinnen und Bewohner des Mehrfamilienhauses, in dem er lebt, Kenntnis von diesem personenbezogenen Datum erlangen.

Datenschutzrechtlich ist das beschriebene Vorgehen nicht zu beanstanden, da es sich lediglich um eine fortlaufende Ordnungsnummer handelt, der keinerlei personenbezogene Informationen, wie beispielsweise das Geburtsdatum oder Bestandteile des Namens, zu entnehmen ist. Die im Adressfenster sichtbaren Angaben sind für die Abläufe des Beitragsservice auch unverzichtbar. Nur auf diese Weise können die unzustellbaren Briefe, die eine erhebliche Größenordnung einnehmen, automatisiert und ohne Öffnung des Briefes dem jeweiligen Beitragskonto bzw. Aktenzeichen zugewiesen und die Tatsache der Unzustellbarkeit vermerkt werden.

Entsprechend sehen es auch die Landesdatenschutzbeauftragten von Hessen und Berlin, die bereits im Jahre 1996 schriftlich bestätigt haben, dass es sich bei der Beitragsnummer um kein personenbezogenes Datum handelt.

Die vom Petenten skizzierte Gefahr, dass die sichtbare Beitragsnummer in unberechtigter Weise genutzt werden könnte, um sich einer bestehenden Zahlungspflicht zu entziehen, dürfte sich – wenn überhaupt – nur in sehr seltenen Ausnahmefällen realisieren können. Denn in der Regel existiert für jede Wohnung ein eigener Briefkasten, so dass eine Kenntnisnahme durch unberechtigte Dritte in der Praxis kaum vorkommen dürfte.

2. Überprüfung der Informationssicherheit bei der Creditreform Mainz Albert & Naujoks KG

Die Überprüfung der Informationssicherheit der Creditreform Mainz Albert & Naujoks KG, die von den Landesrundfunkanstalten beauftragt worden ist, rückständige Rundfunkgebühren bzw. Rundfunkbeiträge gegenüber den betroffenen Rundfunkteilnehmerinnen und Rundfunkteilnehmern geltend zu machen, dauert an.

Im Nachgang zum Versand des nahezu 800 Seiten umfassenden IT-Sicherheitskonzepts an die prüfenden Landesdatenschutzbeauftragten von Berlin, Bremen, Brandenburg und Hessen haben wir am 29. Oktober 2014 ergänzende Unterlagen verschickt. Eine Stellungnahme der Landesdatenschutzbeauftragten hat uns im Anschluss noch nicht erreicht.

3. Klärungsschreiben des Beitragsservice an Flüchtlingsunterkünfte

Der Presse war zu entnehmen, dass sogenannte Klärungsschreiben des Beitragsservice an Flüchtlinge verschickt werden, mit denen diese um weitergehende Informationen zu einer etwaigen Beitragspflicht gebeten werden. Die damit verbundenen negativen Schlagzeilen überraschen nicht.

Das Vorgehen des Beitragsservice folgt der Logik des dahinterliegenden Mechanismus: Die Flüchtlinge werden mit der Adresse von Flüchtlingsheimen und Auffangstellen bei den Einwohnermeldeämtern gemeldet. Von dort aus geht eine entsprechende Information an den Beitragsservice. Aus diesen Mitteilungen geht allerdings nicht hervor, dass es sich um Flüchtlinge handelt.

Um der schädlichen Berichterstattung so schnell wie möglich zu begegnen, hat sich die Juristische Kommission von ARD, ZDF und Deutsch-



landradio dieser Thematik angenommen. Die Justizariate der einzelnen Häuser versuchen, Namen von Ansprechpartnern aus den Lagezentren der jeweiligen Bundesländer zu erhalten, damit auf diesem Wege die Adressen der Unterkünfte bekannt werden, um sie anschließend sperren zu können.

Auch wenn sich die Nachfrage nach einem Ansprechpartner bzw. einer generellen Übersicht der Unterkünfte aus naheliegenden Gründen als schwierig erwies, konnten die gewünschten Informationen über das Sozialressort, das die Unterbringung der Flüchtlinge in Bremen koordiniert, recherchiert werden. Auf diese Weise war es möglich, die Adressen von Landeserstaufnahmestellen sowie von Flüchtlings- bzw. Asylbewerberheimen dem Beitragsservice zu übermitteln, damit diese für weitere Maßnahmen gesperrt werden.

F. Datenschutz im Informationsverarbeitungszentrum (IVZ)

Als Gemeinschaftseinrichtung betreiben der Norddeutsche Rundfunk, der Mitteldeutsche Rundfunk, der Saarländische Rundfunk, der Rundfunk Berlin-Brandenburg, das Deutschlandradio, Radio Bremen, der Westdeutsche Rundfunk und die Deutsche Welle das rechtlich unselbstständige Informationsverarbeitungszentrum (IVZ).

Dort werden für die beteiligten Anstalten Aufgaben der elektronischen Datenverarbeitung wahrgenommen und durchgeführt. Für die Kontrolle des Datenschutzes und der Datensicherheit sind die Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig.

Am 25. November 2014 fand beim IVZ das jährliche Treffen der Datenschutzbeauftragten der beteiligten Anstalten sowie der zuständigen Mitarbeiterinnen und Mitarbeiter des IVZ statt, an dem ich urlaubsbedingt nicht teilnehmen konnte. Anhaltspunkte, die ein Tätigwerden der Datenschutzbeauftragten erfordert hätten, haben sich dabei nicht ergeben.

G. Weitergehende Aktivitäten des Datenschutzbeauftragten

1. Sitzungen des AK DSB

Auch in diesem Berichtszeitraum fanden wieder zwei turnusmäßige Sitzungen des AK DSB statt.

Ziel dieses Kreises ist es, Erfahrungen und Meinungen zu datenschutzrechtlichen Problemen in den Rundfunkanstalten auszutauschen und den Datenschutz beim Rundfunkbeitragseinzug sowie bei Gemeinschaftsprojekten zu koordinieren. Darüber hinaus begleitet der Arbeitskreis auch die gesetzgeberischen Aktivitäten, sofern Fragen des Datenschutzes und der Datensicherheit im Rundfunk betroffen sind.

Einen thematischen Schwerpunkt einer Sitzung des AK DSB bildeten die datenschutzrechtlichen Anforderungen beim Betrieb von HbbTV. Dieser Standard für Hybrid-TV ermöglicht es den Programmanbietern, zusätzliche Informationen sowohl über das Fernsehsignal als auch über eine Internetverbindung anzuzeigen. Durch HbbTV findet also eine inhaltliche Verknüpfung von Rundfunk- und Internetinhalten statt.

Das bedeutet auch, dass die sogenannte IP-Adresse bei der Nutzung des entsprechenden Fernsehgerätes übertragen werden muss, um Inhalte aus dem Internet anzeigen zu können. Dabei handelt es sich um ein personenbezogenes Datum, so dass auch die datenschutzrechtlichen Bestimmungen beachtet werden müssen.

Ein weiterer Schwerpunkt der Arbeit des AK DSB bildeten die datenschutzrechtlichen Fragestellungen im Zusammenhang mit der Evaluation des RBStV (siehe meine Ausführung unter C. 3).

2. Vertretung des AK DSB in der europäischen Datenschutzgruppe nach Art. 29 EU-Datenschutzrichtlinie

Art. 29 Abs. 2 EU-Datenschutzrichtlinie sieht die Einsetzung einer Europäischen Datenschutzgruppe vor, die aus Vertretern der einzelnen Mitgliedsstaaten der EU besteht. Diese Gruppe berät die EU-Kommission und trägt zur einheitlichen Anwendung der Datenschutzrichtlinie in den EU-Staaten bei. Seit Ende 2001 ist eine Vertreterin bzw. ein Vertreter des AK DSB an der Gruppe beteiligt. Dies ist nach wie vor der Datenschutzbeauftragte des Norddeutschen Rundfunks.

Dadurch ist eine regelmäßige Information der Landesrundfunkanstalten über die sich abzeichnende Entwicklung und Meinungsbildung im Bereich des Datenschutzes auf europäischer Ebene sichergestellt.

3. Teilnahme an Fortbildungen und Veranstaltungen

Am 15./16. Juni 2015 habe ich an der Jahresfachkonferenz Datenschutz und Datensicherheit 2015 in Berlin teilgenommen. Dort trafen sich über 170 Datenschutzbeauftragte, Anwälte und IT-Sicherheitsverantwortliche zum Gedanken- und Erfahrungsaustausch.

Am 17. und 18. Juni 2015 veranstalteten die ARD.ZDF medienakademie und das Institut für Rundfunktechnik (IRT) beim Rundfunk Berlin-Brandenburg in Berlin das Symposium "Big Data - Produktiver Mehrwert oder unberechenbare Datenflut?" Der Umgang mit großen Datenmengen



ist im Rundfunk grundsätzlich nichts Neues, neu ist allerdings die Bedeutung von Daten als Faktor für die Wertschöpfung.

Am 6./7. Oktober 2015 habe ich an dem Seminar „IT-Grundlagen für Datenschutzbeauftragte“ teilgenommen. Dort ging es um die Vermittlung von Basiswissen und um das Aufzeigen von neueren Entwicklungen im Bereich der Informationstechnologie.

Bremen, 31.Oktober 2015

Gezeichnet

Sven Carlson