Tätigkeitsbericht

des Datenschutzbeauftragten des

Hessischen Rundfunks

Ulrich Göhler

für den Zeitraum

01. Januar 2014 bis 31. Dezember 2015

Gliederung:

Zusammenfassung

- Obwohl das Hessische Datenschutzgesetz einen Tätigkeitsbericht des Datenschutzbeauftragten des Hessischen Rundfunks nicht vorsieht, wird seit Mitte 2006 wieder ein Tätigkeitsbericht erstellt und auf den Internetseiten des Hessischen Rundfunks veröffentlicht.
- Wie in den Vorjahren habe ich im Berichtszeitraum wieder eine Reihe von Stellungnahmen zu hr-internen Projekten und Verfahrenserweiterungen abgegeben. Auch wurden Verfahrensverzeichnisse (§ 6 HDSG) neu erstellt oder aktualisiert und dem Personalrat im Rahmen der Mitbestimmung vorgelegt.
- Die Zahl der Beschwerden und Eingaben zum Datenschutz ist in den letzten Jahren weiterhin rückläufig. Förmliche Beanstandungen wegen Verletzungen des Datenschutzes brauchten im Berichtszeitraum nicht ausgesprochen zu werden. Letztlich konnten alle Sachverhalte einvernehmlich geregelt werden.
- Der Arbeitskreis Datenschutzbeauftragte ARD/ZDF/DLR (AK DSB) ist weiterhin ein wesentlicher Baustein bei der Koordinierung und Abstimmung der rechtlichen Bewertungen und von durchzuführenden Datenschutzmaßnahmen der Landesrundfunkanstalten.

1. Vorbemerkung/Organisation

In der Sitzung des Rundfunkrates des Hessischen Rundfunks vom 16. November 2012 wurde ich mit Wirkung zum 1. Januar 2013 für weitere fünf Jahre zum Datenschutzbeauftragten für den journalistisch-redaktionellen Bereich gemäß § 37 Abs. 2 HDSG bestellt. Ebenfalls für die Dauer von weiteren fünf Jahren und mit Wirkung zum 1. Januar 2013 wurde mir gemäß § 5 Abs. 1 HDSG vom Intendanten des Hessischen Rundfunks mit Schreiben vom 19. Dezember 2012 die Funktion des betrieblichen Datenschutzbeauftragten bis zum 31. Dezember 2017 übertragen.

In Anwendung von § 37 Abs. 3 HDSG und in Übereinstimmung mit der bisher geübten Praxis wird beim Hessischen Rundfunk sowohl die Funktion des betrieblichen Datenschutzbeauftragten als auch die des für den journalistisch-redaktionellen Bereich zuständigen Datenschutzbeauftragten von mir in Personalunion ausgeübt. Ich nehme diese Aufgabe neben meiner Tätigkeit als Mitarbeiter der Internen Revision wahr. Eine fallweise Unterstützung erfahre ich hierbei durch eine Sachbearbeiterin der Revision.

Analog der Verfahrensweise der Vorjahre wird dieser Tätigkeitsbericht vorgelegt und im Internet veröffentlicht, obwohl das HDSG seit 1986 einen solchen Bericht des Datenschutzbeauftragten des Hesssichen Rundfunks nicht mehr vorsieht.

Um als unabhängige Kontrollstelle i. S. von Artikel 28 Abs. 5 der EU-Datenschutzrichtlinie anerkannt werden zu können und um ein Vertragsverletzungsverfahren der EU-Kommission zu vermeiden, wird gleichwohl seit 2006 wieder ein Tätigkeitsbericht des hr-Datenschutzbeauftragten vorgelegt.

Der vorliegende Tätigkeitsbericht betrifft den Zeitraum vom 1. Januar 2014 bis 31. Dezember 2015. Es werden darin allgemeine Entwicklungen des Datenschutzes sowie datenschutzrechtlich relevante Veränderungen und Problemstellungen im Hessischen Rundfunk während des Berichtszeitraums dargestellt.

2. Entwicklung des Datenschutzrechts

2.1 Europa

2.1.1 EU-Datenschutz-Grundverordnung (EU-DSGVO)

In meinem letzten Tätigkeitsbericht hatte ich darüber berichtet, dass auf Basis eines Vorschlages der Europäischen Kommission die momentan noch gültige „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (EU-Datenschutzrichtlinie) aus dem Jahre 1995 einer grundlegenden Überarbeitung unterzogen werden sollte.

Nachdem von der Europäischen Kommission gegen Ende des Jahres 2011 der Entwurf einer Datenschutz-Grundverordnung (EU-DSGVO) vorgelegt worden war, kam das Vorhaben bei den Verhandlungen mit dem Rat der Europäischen Union (EU-Ministerrat) sowie dem Europäischen Parlament erheblich in's Stocken – eine schnelle Einigung war zunächst nicht in Sicht.

Aber, wie so oft auf der (europäischen) politischen Ebene, können Vorhaben, bei denen niemand mit einer schnellen Realisierung rechnet, die aber einen gewissen „Reifegrad" erreicht haben, plötzlich doch ganz schnell verabschiedet und umgesetzt werden. So auch geschehen im Fall der EU-DSGVO.

Nach zähen Verhandlungen haben die Verhandlungsführer des Trilogs zwischen Europäischem Parlament, EU-Kommission und EU-Ministerrat nach knapp vier Jahren, Ende 2015, den Text der lang erwarteten Datenschutz-Grundverordnung verabschiedet. Eine am 15. Dezember 2015 zwischen Parlament und Rat informell erzielte Einigung wurde am 17. Dezember 2015 vom Innen- und Rechtsausschuss des Parlaments mit großer Mehrheit angenommen. Voraussichtlich im März oder April 2016 soll hierüber im EU-Parlament abgestimmt werden. Nach Inkrafttreten der Verordnung (voraussichtlich 2018) haben die Mitgliedsstaaten zwei Jahre Zeit zur Umsetzung.

Da es sich um eine **Verordnung** handelt, gelten die Regelungen unmittelbar auch für Deutschland. Insoweit wird die EU-DSGVO auch für das deutsche Datenschutzrecht weitreichende Auswirkungen haben. Das BDSG zum Beispiel wird im jetzigen Inhalt weitgehend aufgelöst, auch die Datenschutzgesetze auf Landesebene bedürfen einer entsprechenden Anpassung.

2.1.2 EuGH – Urteil zu „Safe Harbor“

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.

Das 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 Datenschutzbeauftragter 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 den Hessischen Rundfunk haben dürfte. 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.

2.2 Bundesrecht

2.2.1 IT-Sicherheitsgesetz

Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz) ist am 25. Juli 2015 in Kraft getreten. Durch das Gesetz werden sowohl das BSI-Gesetz als auch andere Gesetze wie z.B. das Telemediengesetz oder das Telekommunikationsgesetz geändert.

Das IT-Sicherheitsgesetz führt eine obligatorische Meldepflicht für „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit“ (= IT-Sicherheitsvorfälle) ein. Zusätzlich werden Mindeststandards „nach dem Stand der Technik“ für die IT-Sicherheit bei den Betreibern kritischer Infrastrukturen festgelegt und die Unternehmen bzw. Organisationen sind verpflichtet, alle zwei Jahre nachzuweisen, dass die Sicherheitsanforderungen erfüllt sind

Mit dem IT-Sicherheitsgesetz sollen Betreiber sogenannter „kritischer Infrastrukturen“ u.a. verpflichtet werden, ihre IT-Infrastrukturen besser vor Hacker-Angriffen zu schützen. Welche Unternehmen bzw. Organisationen konkret unter den Begriff der „kritischen Infrastrukturen“ fallen werden, wird in einer noch zu erlassenden Rechtsverordnung geregelt werden. Gemäß IT-Gesetz sind hiervon gegenwärtig erfasst die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen sowie generell Einrichtungen „von hoher Bedeutung für das Funktionieren des Gemeinwesens“.

Obwohl die einzelnen Landesrundfunkanstalten – wie z.B. der Hessische Rundfunk – sicherlich eine „hohe Bedeutung für das Funktionieren des Gemeinwesens“ haben, ist davon auszugehen, dass die Rundfunkanstalten nicht den o.g. „kritischen Infrastrukturen“ zuzurechnen sind. Da die Landesrundfunkanstalten nicht der Gesetzgebungskompetenz des Bundes unterliegen, sind sie vom BSI-Gesetz und seinen Regelungen ausgenommen. Gleichwohl ist nicht auszuschließen, dass neben den Regelungen des Bundes auch entsprechende landesgesetzliche Bestimmungen erlassen werden.

2.2.2 Vorratsdatenspeicherung

Am 16. Oktober 2015 hat der Deutsche Bundestag das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ verabschiedet.

Telekommunikationsunternehmen werden dadurch verpflichtet, Internet- und Verkehrsdaten jedes Bürgers anlasslos für zehn Wochen zu speichern. Standortdaten sind vier Wochen zu speichern, Nutzungsinhalte dagegen müssen nicht erfasst werden.

Einen ersten Versuch für ein entsprechendes Gesetz 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. Allerdings verstößt eine Vorratsdatenspeicherung auch nach Ansicht des BVerfG nicht grundsätzlich gegen das Grundgesetz.

Das damalige Gesetz zur Vorratsdatenspeicherung basierte auf einer entsprechenden EU-Richtlinie, die jedoch am 8. April 2014 vom EuGH für ungültig erklärt worden war. Mit dem Wegfall der europäischen Grundlage war auch die Bundesregierung zunächst von ihrem Vorhaben abgerückt, schnell ein neues Gesetz zur Vorratsdatenspeicherung auszuarbeiten. Gleichwohl haben die Koalitionspartner von CDU/CSU und SPD nunmehr das entsprechende Gesetz erlassen.

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.

Ob dieses Gesetz die damit verfolgten Ziele der effektiven Bekämpfung der Kriminalität und des Terrorismus tatsächlich erreicht, ist nach wie vor sehr fraglich. Darüber hinaus haben nach Inkrafttreten des Gesetzes einige Bundestagsabgeordnete sowie Journalisten- und Medienverbände beim BVerfG eine einstweilige Anordnung beantragt. Damit soll erreicht werden, dass die Speicherfrist der Telekommunikationsanbieter bis zur Entscheidung über eine Verfassungsbeschwerde ausgesetzt wird.

3. Datenschutz im Hessischen Rundfunk

Auch für die zwei zurückliegenden Jahre kann ich den in meinen vorhergehenden Tätigkeitsberichten geäußerten positiven Eindruck bestätigen, dass bei innerhalb des Hessischen Rundfunks auftretenden datenschutzrechtlichen Fragestellungen in der ganz großen Mehrheit der Fälle eine frühzeitige Einbindung des Datenschutzbeauftragten gewährleistet ist.

Diese frühzeitige Einbindung wird u. a. durch die seit Jahren praktizierte direkte Mitarbeit und Beteiligung des Datenschutzbeauftragten in den unterschiedlichsten Projekt-, Arbeits- und Lenkungsgruppen sichergestellt. Auch durch die von mir selbst mehrmals im Jahr durchgeführten Schulungen zum Thema Datenschutz (Auszubildende, IT-Mitarbeiter/innen, neue Mitarbeiter/innen etc.) wird das im hr vorhandene Datenschutzbewusstsein weiter gestärkt bzw. ständig in Erinnerung gerufen. So kann bei fast allen Mitarbeiterinnen und Mitarbeitern ein recht hohes Bewusstsein für datenschutzrechtliche Sachverhalte konstatiert werden.

Die im Folgenden exemplarisch aufgeführten Einzelfälle werden analog der in meinen letzten Tätigkeitsberichten gewählten Darstellungsweise getrennt nach den Bereichen „Allgemeines/Verwaltung“ sowie „Programm- und Produktionsbereich“ betrachtet und zeigen die Bandbreite der zu bearbeitenden Themen auf.

3.1 Allgemeines/Verwaltung

3.1.1 Einführung einer neuen Telefon-Anlage

Die beim Hessischen Rundfunk seit mehr als 20 Jahren im Einsatz befindliche Telefonanlage musste ersetzt werden, da zum einen die veraltete Technik vom Hersteller nicht mehr unterstützt wurde und zum anderen generell eine neue Systemplattform mit zeitgemäßen und wirtschaftlichen Kommunikationsmöglichkeiten zur Verfügung gestellt werden sollte.

Da beim Betrieb einer Telefonanlage u.a. auch personenbezogene Daten verarbeitet werden, wurde ich als Datenschutzbeauftragter von Anfang an in das entsprechende Projekt mit einbezogen. Anfangs als „Gast“ im Rahmen der jeweiligen Projektgruppensitzungen, später dann als Mitglied der zur Projektsteuerung eingesetzten Lenkungsgruppe.

Weil die neue, zeitgemäße Telefonanlage auf der sogenannten „Voice over IP“[1]-Technologie basiert, mussten bei der Einführung vor allem auch Aspekte der Daten- bzw. IT-Sicherheit beachtet werden. Beispielsweise ist es potentiellen Angreifern aufgrund der eingesetzten Technik möglich, die über das Netzwerk übertragenen Sprach-Datenpakete abzugreifen und die Gespräche aufzuzeichnen.

Darüber hinaus bietet eine derartige Telefonanlage eine Vielzahl an Möglichkeiten zur Systemkonfiguration sowie der Bedienung durch die Nutzer/innen. Deswegen ist darauf zu achten, dass sowohl die (Grund)Einstellungen des Systems in datenschutzrechtlich zulässiger bzw. wünschenswerter Weise vorgenommen werden als auch die den Nutzer/innen zur Verfügung stehenden Funktionalitäten bzw. Leistungsmerkmale möglichst datenschutzfreundlich gestaltet sind.

Die Gewährleistung der Daten-/IT-sicherheitstechnischen Kriterien wurde dadurch sichergestellt, dass zum einen eine enge und ständige Einbeziehung meiner Person und auch des IT-Sicherheitsmanagers des Hessischen Rundfunks erfolgte. Zum anderen wurden die im Leistungskatalog definierten Kriterien bzgl. Datensicherheit und Verschlüsselung sowohl durch hr-interne Experten als auch durch externe Dienstleister kontinuierlich durch entsprechende Audits auf Einhaltung überprüft.

Aufgrund der Vielfalt der Konfigurationsmöglichkeiten einer solchen Telefonanlage lauten die aus Sicht des Datenschutzes an ein solches System zu stellenden Forderungen insbesondere „Transparenz“ und „Selbstbestimmung“. Diese Forderungen wurden im Wesentlichen dadurch umgesetzt, dass zum einen die während eines Telefonats gerade aktivierten Leistungsmerkmale (z.B. Anzahl Teilnehmer in der Konferenz, Übermittlung der Rufnummer etc.) sämtlichen Gesprächspartnern angezeigt werden und zum anderen entsprechende Leistungsmerkmale von den Nutzern der Anlage individuell (teilweise von Telefonat zu Telefonat) eingestellt, freigegeben oder auch gesperrt werden können.

Die von den Nutzer/innen selbst einstellbaren Leistungsmerkmale sowie der generelle Umgang mit der neuen Telefonanlage wurde den Nutzer/innen anhand von im hr-Intranet zur Verfügung gestellten „videotutorials“ erläutert, so dass auch hier dem datenschutzrechtlichen Gebot der Transparenz und Selbstbestimmung Rechnung getragen wurde.

[1] IP = Internet Protocol; Adresse in Computernetzen, die Geräten zugewiesen wird, die an das Netz angebunden sind; dadurch können die Geräte eindeutig identifiziert und adressiert werden.

3.1.2 Einführung eines „Internen Arbeitsmarktes“ (IAM)

In meinem letzten Tätigkeitsbericht hatte ich über die Einführung eines Systems für Online-Bewerbungen (E-recruiting) berichtet. Auf Basis einer von der Firma SAP angebotenen Lösung werden mithilfe dieses elektronischen Bewerbungssystems die von externen Bewerber/innen eingehenden Bewerbungen fast ausschließlich elektronisch verarbeitet. Dies führt einerseits zu einer Reduzierung des hr-internen manuellen Barbeitungsaufwandes und andererseits kann den Bewerber/innen eine zeitgemäßere Form der Bewerbung angeboten werden.

Basierend auf den hierbei gemachten positiven Erfahrungen für externe Bewerbungen sollte nun auch ein für interne Bewerbungen geignetes Verfahren/System gefunden werden. Die Einrichtung eines solchen internen Arbeitsmarktes soll es dem Hessischen Rundfunk ermöglichen, die intern vorhandenen Potenziale von festen und freien Mitarbeiter/innen optimal einzusetzen, ganz im Sinne von „die richtigen Mitarbeiter/innen zum richtigen Zeitpunkt am richtigen Ort.“ Darüber hinaus soll durch den Einsatz eines derartigen, relativ einfach zu handhabenden Systems generell die Wechselbereitschaft sowie das Interesse an der Übernahme neuer Aufgaben gesteigert werden. Diese Aspekte erlangen zunehmend Bedeutung in einem von Spar- und Konsolidierungserfordernissen geprägten Umfeld mit entsprechenden Auswirkungen auf die Personalkapazitäten und Stellenanforderungen.

Letztendlich wurde der IAM auf Basis des ebenfalls beim E-recruiting eingesetzten SAP-Moduls realisiert und kann über das Intranet genutzt werden.

Im IAM ist es sowohl möglich, konkrete Stellenangebote einzustellen, auf die sich dann die interessierten festangestellten und freien Mitarbeiter/innen auf elektronischem Wege bewerben können, als auch sozusagen „auf Verdacht“ sein eigenes Bewerberprofil zu hinterlegen und damit Interesse an neuen Aufgaben zu bekunden, damit die eigene Person bei entsprechenden Gesuchen gleich berücksichtigt werden kann.

Analog zum „E-recruting“ wird daher auch beim IAM eine Vielzahl von personenbezogenen Daten verabreitet. Die hierbei wichtigsten Forderungen aus Datenschutzsicht sind neben der generellen Zulässigkeit des Verfahrens insbesondere die Forderung nach „Transparenz des Verfahrens“, das „Gebot der Freiwilligkeit“ (der Teilnahme am Verfahren) sowie das „Erfordernis der Einwilligung der Teilnehmenden in das Verfahren“.

Im Rahmen der Einführung des IAM wurde deutlich kommuniziert, dass es keine verpflichtende Teilnahme gibt. Das Einstellen eines Bewerberprofils bzw. die Bewerbung auf eine Stellenausschreibung erfolgt ausschließlich auf freiwilliger Basis.

Die Einwilligung der Mitarbeiter/innen wird – ebenfalls analog zum E-recruiting – dadurch eingeholt, dass bereits bei der Registrierung ein Hinweis auf die im System hinterlegte (und verpflichtend zur Kenntnis zu nehmende) Datenschutzerklärung erfolgt, in der der Umgang mit den personenbezogenen Daten erläutert wird. Das datenschutzrechtliche Gebot der Datensparsamkeit wird beispielsweise dadurch sichergestellt, dass bei der Registrierung lediglich wenige Felder als Pflichtfelder definiert wurden; auch im Verlauf der Bewerbung bzw. bei Einstellung des Bewerberprofils erforderliche Eingaben werden auf ein Minimum beschränkt, in dem z.B. vom Hersteller eigentlich vorgesehene Felder ausgeblendet bzw. gelöscht wurden.

Schließlich stellt ein striktes Rollen- und Berechtigungskonzept sicher, dass lediglich hierzu berechtigte Personen die Bewerberprofile und Bewerbungen einsehen bzw. anlegen können.

3.1.3 Installation einer „Kontakt-Datenbank“ (KoDa) für den Hörer- und Zuschauerservice (HZS)

Die Kunden des Hessischen Rundfunks (Zuschauer des hr-Fernsehens, Hörer der hr-Radiowellen, Nutzer des Online-Angebots, Konzertbesucher/-abonnenten etc.) wenden sich über diverse Kommunikationswege (Telefon, E-Mail, Brief etc.) an den hr. Die „zentrale Anlaufstelle“ ist hierbei der sogenannte „Hörer- und Zuschauerservice“, kurz „HZS“. Um die Vielfalt der Anfragen bewältigen zu können, wird eine Datenbank verwendet, die u.a. aufgrund nicht mehr existenter Unterstützung seitens des Herstellers abgelöst werden musste.

Die neue Datenbank wurde von der IT des Hessischen Rundfunks selbst entwickelt und auf den einfachen Namen „**Ko**ntakt-**Da**tenbank“ (= KoDa) getauft. Da mithilfe einer solchen Datenbank vielfältige personenbezogene Daten verarbeitet werden (können), war auch hier meine Einbeziehung erforderlich. Diese erfolgte sowohl durch beratende Gespräche im Vorfeld als auch durch entsprechende Systemdemonstrationen nach Fertigstellung, aber vor Inbetriebnahme der KoDa.

Wichtig war aus datenschutzrechtlicher Sicht u.a., dass die Kunden, die sich mit ihrem Anliegen an den Hessischen Rundfunk wenden, darüber in-

formiert werden, dass – sofern erforderlich - ihre personenbezogenen Daten zur Bearbeitung der Anfrage gespeichert werden. Im Fall von Standardsachverhalten wie „Äußerung von Lob/Kritik/Meinung“, „Nachfrage zu einer Sendung“ oder „Fragen allgemeiner Art“ werden jedoch keinerlei personenbezogene Daten erfasst.

Insgesamt sind jedoch nur wenige Felder für personenbezogene Daten vorgesehen, wie z.B. „Vor-Nachname“, „Anschrift“, „Telefon“ oder „E-Mail-Adresse“. Die Daten werden nach Ablauf von sechs Monaten gelöscht.

Dieser Zeitraum ergibt sich dadurch, dass Kunden, die sich mehrfach wegen eines oder unterschiedlicher Anliegen an den Hessischen Rundfunk wenden, offenbar häufiger beim HZS beschweren, warum ihre Daten schon wieder aufgenommen werden und sie ihre Einwilligung zur Verarbeitung geben sollten - schließlich müssten die Daten doch noch von der letzten Anfrage vorliegen!

Die Festlegung auf sechs Monate Speicherdauer für die Daten versucht hier, einen Kompromiss zu finden zwischen dem gesetzlichen Erfordernis der unverzüglichen Löschung der Daten, sofern diese nicht mehr für den Zweck benötigt werden, für den sie erhoben wurden (Vgl. § 19 Abs. 3 HDSG) und dem Interesse der Kunden, ihre Daten nicht jedes Mal neu angeben zu müssen.

3.2 Datenschutz im Programm- und Produktionsbereich

Einführung einer „Multimedialen Produktions-App“ (muPROApp)

Von den Reportern der Rundfunkanstalten wird in zunehmendem Maße eine cross-/bzw. multimediale Arbeitsweise gefordert. Dies bedeutet z.B., dass nicht nur Material (Fotos, Videos, O-Töne etc.) am Ort des Geschehens aufgezeichnet wird und möglichst schnell an die Rundfunkanstalt übermittelt werden muss, sondern beispielsweise auch, dass Reporter für Live-Gespräche mit den Moderatoren zur Verfügung stehen sollen. Die Aufzeichnung und Übermittlung des Materials sowie das Führen von Live-Gesprächen erfolgt bevorzugt mit Hilfe mobiler Endgeräte (Smartphone, Laptop). Die hierfür erforderlichen Funktionalitäten werden üblicherweise durch eine geeignete (Software-) Anwendung bereitgestellt.

Aus diesem Grund sollte ARD-weit ein einheitliches „Multifunktionswerkzeug“ geschaffen werden, um genau diese Anforderungen erfüllen zu können. Daher wurde die Entwicklung der sogenannten „multimedialen Produktions-App“ (=muPROApp) vorgenommen. Mithilfe dieser App soll vom Reporter zur Verfügung gestelltes Material an einen Server im ARD-Sternpunkt in Frankfurt übermittelt und von dort an die sendende(n) Rundfunkanstalt(en) „weitergeleitet“ werden. Im ersten Schritt geht es darum, die Audio-Funktionalitäten zu nutzen; im zweiten Schritt sollen dann die Video-Funktionalitäten hinzukommen.

Da diese muPROApp dazu dient, Audio- bzw. Videoinhalte zu übermitteln, werden hier zwar auch personenbezogene Daten verarbeitet, diese unterfallen jedoch dem sogenannten „Medienprivileg“. Die Verarbeitung der Daten erfolgt ausschließlich zu „eigenen journalistisch-redaktionellen Zwecken“. Gemäß § 3 Abs. 5 Satz 1 HDSG sind demzufolge im Wesentlichen nur Vorschriften zur Daten**sicherheit** zu berücksichtigen.

Die Einhaltung der Vorgaben auf technischer Seite wurde zum einen sichergestellt durch die enge Einbindung der jeweils zuständigen IT-Sicherheitsbeauftragten sowie zum anderen durch die Zertifizierung der implementierten Sicherheitsmaßnahmen durch den TÜV-Rheinland.

Die Einhaltung der Vorgaben auf Seiten der Nutzer/Reporter hingegen konnte und kann nur sichergestellt werden, wenn hr-eigene Smartphones genutzt werden. Diese werden von der IT des Hessischen Rundfunks zentral verwaltet und z.B. automatisch mit entsprechenden Sicherheitsupdates versehen. Bei den privaten Geräten der Nutzer/Reporter kann dies jedoch nicht gewährleistet werden, da diese privaten Geräte dem direkten Einflussbereich des Hessischen Rundfunks entzogen sind und somit z.B. die Ausstattung mit der jeweils aktuellsten Sicherheitssoftware in den Verantwortungsbereich des jeweiligen Nutzers/Reporters gestellt ist.

In meiner Stellungnahme habe ich darauf hingewiesen, dass auf den von den Reportern eingesetzten privaten mobilen Endgeräten sehr häufig das tool „*WhatsApp*“ installiert ist. Mithilfe dieses tools können zwar auf sehr einfache Weise Textnachrichten, Bilder oder Videos mit anderen *WhatsApp*-Nutzern ausgetauscht werden, aber das tool greift auch in regelmäßigen Abständen auf die unter den Kontakten auf dem mobilen Endgerät gespeicherten Telefonnummern zu.

Damit sind die auf dem privaten Smartphone gespeicherten Kontakte/Telefonnummern nicht mehr „privat“, d.h. nur dem Nutzer des Smartphones bekannt, sondern werden auf US-amerikanischen Servern und/oder in der „cloud“ verarbeitet. Eine Sicherstellung des u.a. für Reporter wichtigen „Informantenschutzes“ ist damit nicht mehr möglich.

Da diese Problematik aber generell den Umgang mit mobilen Endgeräten betrifft, egal ob beruflich oder privat, habe ich der Einführung der muPROApp gleichwohl zugestimmt. Vereinbart wurde, die betreffenden Reporter durch geeignete Maßnahmen (Schulungen, Infoveranstaltungen, Aushändigung von Merkblättern) für das Thema zu sensibilisieren und dadurch zumindest in gewissem Umfang die Gewährleistung des „Informantenschutzes" sicherzustellen.

3.3 Diverse Sachverhalte (Verwaltung und Programm)

Weitere bearbeitete Themen werden im Folgenden lediglich in Stichworten aufgeführt, da es sich entweder um immer wiederkehrende „Routine-aufgaben" oder um Themen von geringerem Umfang handelt:

- In zahlreichen Fällen werde ich als Datenschutzbeauftragter quasi „routinemäßig" eingebunden, sobald Aktualisierungen oder Änderungen bei einmal implementierten IT-Programmen erfolgen. Die Mitarbeiter/innen der IT sind durch die jahrelange Zusammenarbeit mit dem Datenschutzbeauftragten im Regelfall dafür „sensibilisiert", eine frühzeitige Einbindung des Datenschutzbeauftragten sicherzustellen, da hierdurch zeitlicher Druck bei entsprechenden Antragstellungen vermieden werden kann und die datenschutzrechtlich erforderliche Dokumentation („Verfahrensverzeichnisse") relativ aktuell gehalten wird.
- Meine Beteiligung ist normalerweise ebenfalls sichergestellt, wenn es um die Implementierung von „kleineren Software-tools" geht, die gleichwohl über einen sogenannten „Antrag auf Inbetriebnahme" beim Hessischen Rundfunk eingeführt werden sollen. So beispielsweise geschehen im Fall der Erweiterung eines Programms für das Gebäudemanagement um ein Modul zur Bearbeitung von Störungsmeldungen sowie bei der Einführung einer elektronischen Schließanlage zur Sicherung von Räumlichkeiten, die besondere Sicherheitsanforderungen erfüllen müssen. Da in solchen Fällen auch personenbezogene Daten wie beispielsweise „Vorname/Name", „Telefonnummer", „E-Mail-Adresse" oder „Personalnummer" verarbeitet werden, werde ich im Rahmen der sogenannten Vorab-Kontrolle gemäß § 7 Abs. 6 HDSG eingebunden.

- Auch vom Hessischen Rundfunk werden bereits seit mehreren Jahren sogenannte „Apps“ angeboten. Dabei handelt es sich um kleine Programme für z.b. Smartphones oder Tablets, mit denen man beispielsweise die hr-Radiowellen empfangen kann und aktuelle Informationen zu Wetter, Verkehr und Nachrichten erhält. Bei der Entwicklung dieser „Apps“ müssen ebenfalls datenschutzrechtliche Anforderungen berücksichtigt werden, da es u.a. darum geht, die Apps mit möglichst datenschutzfreundlichen Einstellungen zu gestalten, die Nutzer/innen über den Umgang mit ihren personenbezogenen Daten aufzuklären und ggf. Vereinbarungen zur Auftragsdatenverarbeitung abzuschließen, sofern mit externen Dienstleistern zusammengearbeitet wird.
- Bei der Installation von Studio-webcams, mit deren Hilfe ein live-Bild der Moderator/innen in den Hörfunkstudios der Radiowellen über das Internet übertragen wird, gilt es neben Aspekten des Persönlichkeits- und ggf. Urheberrechts auch datenschutzrechtliche Anforderungen zu berücksichtigen. Z.B. sollte die Übertragung möglichst auf freiwilliger Basis erfolgen, d.h. die Moderator/innen sollten immer die Möglichkeit haben, die Übertragung selbst zu beenden. Ausserdem darf es nicht möglich sein, Inhalte, die auf den Monitoren der Moderator/innen dargestellt werden, durch die webcams zu erfassen und schließlich müssen Besucher(gruppen), die sich im Studio befinden, durch entsprechende optische Hinweise über die Aufzeichnung und die damit verbundene Übertragung in’s Internet informiert werden.
- Neben diesen rein datenschutzrechtlichen Fragestellungen war ich auch in Themen eingebunden, die den Datenschutz mindestens berühren. Zum einen war ich tätig als Leiter einer Arbeitsgruppe, die den Auftrag hatte, eine Dienstvereinbarung zum Thema „Durchführung von (IT-)Sicherheitstests“ zu erarbeiten. Gemeinsam mit dem IT-Sicherheitsmanager des hr, der IT-Sicherheitsbeauftragten des ARD-Sternpunkts, einem Vertreter des Gesamtpersonalrats sowie Führungskräften der IT wurden „Standards“ ausgearbeitet, die die Verfahrensweise bei der Durchführung von (IT-)Sicherheitstests festlegen. Darüber hinaus bin ich gegenwärtig noch mit der Leitung einer Arbeitsgruppe betraut, die beauftragt wurde, die bereits existierende Dienstvereinbarung über die Personaldatenverarbeitung mit dem System SAP R/3 HR zu überarbeiten und an die aktuell eingesetzte Version SAP HCM anzupassen.

- Im Rahmen meiner Tätigkeit als Datenschutzbeauftragter erfolgt ebenfalls auf regelmäßiger Basis eine sehr enge Abstimmung mit dem IT-Sicherheitsmanager des hr. In zunehmendem Maße ist es bei der Beurteilung einzelner Sachverhalte erforderlich, neben den Daten**schutz**-Aspekten auch die Daten**sicherheits**-Aspekte zu berücksichtigen. Hier ist aus meiner Sicht die Hinzuziehung von technischem Sachverstand in Person des IT-Sicherheitsmanagers unumgänglich.
- Auch im zurückliegenden Berichtszeitraum habe ich wieder diverse Schulungen zum Thema „Datenschutz" durchgeführt. Diese Schulungen werden generell und verpflichtend durchgeführt für z. B. die jährlich neu eingestellten Auszubildenden sowie im Rahmen einer eintägigen Einführungsveranstaltung für sämtliche neuen Mitarbeiter/innen des Hessischen Rundfunks. Darüber hinaus werden bei Bedarf spezielle Schulungen für neue Mitarbeiter/innen des IT-Bereichs vorgenommen.
- Die Einbindung des Datenschutzbeauftragten erfolgt weiterhin in bewährter Art und Weise „routinemäßig" durch meine Mitarbeit in verschiedenen Arbeits-, Projekt- und Lenkungsgruppen, die datenschutzrechtliche Themenstellungen betreffen.

4. Datenschutz beim Rundfunkbeitrag

Am 1. Januar 2013 ist der Rundfunkbeitragsstaatsvertrag (RBStV) in Kraft getreten. Damit waren einige Änderungen beim bisherigen „Gebühreneinzug“ verbunden. Unter anderem wurde die Gebühreneinzugszentrale (GEZ) umbenannt in „ARD, ZDF Deutschlandradio Beitragsservice“ (zentraler Beitragsservice).

Der im Juni 2015 veröffentlichte Geschäftsbericht des Beitragsservice für das Jahr 2014 weist 44,5 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. Der beim zentralen Beitragsservice geführte Datenbestand umfasste per Ende Dezember 2013 rund 36,4 Millionen Beitragskonten.

Der zentrale Beitragsservice in Köln ist das gemeinsame Rechenzentrum der ARD-Landesrundfunkanstalten, des ZDF und des Deutschlandradios. Es speichert und verarbeitet die für den Rundfunkbeitrag erforderlichen Beitragszahlerdaten im Auftrag der Landesrundfunkanstalten. Datenschutzrechtlich verantwortlich bleibt die jeweils für ein Gebiet zuständige Rundfunkanstalt, für die hessischen Beitragszahlerdaten also der Hessische Rundfunk. Auf die Verarbeitung der hessischen Beitragszahlerdaten ist demnach auch das Hessische Datenschutzrecht anzuwenden, vorrangig aber die bereichsspezifischen Datenschutzregelungen des Rundfunkbeitragsstaatsvertrages (RBStV). Der zentrale Beitragsservice arbeitet datenschutzrechtlich im Auftrag der Landesrundfunkanstalten Die betriebliche Datenschutzbeauftragte des zentralen Beitragsservice arbeitet mit dem/den nach Landesrecht zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese über Verstöße gegen Datenschutzvorschriften und über eingeleitete Maßnahmen.

4.1 Fragen mit direktem Hessen- bzw. hr-Bezug

Einzelfälle (Anfragen, Beschwerden)

Anfragen und Beschwerden zum Datenschutz beim Rundfunkbeitragseinzug haben in Hessen mehrere mögliche Adressaten:

- Sie werden direkt an den **Datenschutzbeauftragten des Hessischen Rundfunks** gerichtet, dessen Name und Adresse u. a. auf den Internet-Seiten des zentralen Beitragsservice zu finden sind.

- Sie werden an den **zentralen Beitragsservice in Köln** geschickt, deren Datenschutzbeauftragte die Eingaben in der Regel in einer ersten Reaktion beantwortet und bei eventuellen Rückfragen dann den Datenschutzbeauftragten der jeweiligen Landesrundfunkanstalt, hier den des Hessischen Rundfunks, einschaltet.

- Eine unbekannte Anzahl von Fragen und Beschwerden gelangt zum **Hessischen Datenschutzbeauftragten**, der diese entweder aus seinem Wissen und der Erfahrung heraus beantwortet und/oder zur Aufklärung des Sachverhaltes den Beitragsservice und/oder den Datenschutzbeauftragten des hr einbezieht.

- Schließlich enthalten die Anfragen und Eingaben zum Rundfunkbeitrag, die direkt an den **Beitragsservice des hr** gesandt werden, oft auch Fragen von datenschutzrechtlicher Relevanz, die dann meist mit mir besprochen werden.

Eingaben an den hr-Datenschutzbeauftragten

Wie in meinen vorangegangenen Tätigkeitsberichten dargestellt, handelte es sich bei der Mehrzahl der an mich gerichteten Eingaben um Beschwerden über das Vorgehen und die Tätigkeit der Rundfunkgebührenbeauftragten. Nachdem dieser Beauftragtendienst im Zuge der Umstellung auf den Rundfunkbeitrag im Sommer 2013 beim Hessischen Rundfunk abgeschafft wurde, haben mich naturgemäß keine derartigen Eingaben mehr erreicht.

Auch der im Zuge der Umstellung erfolgte einmalige Meldedatenabgleich, bei dem die Einwohnermeldeämter einmalig bestimmte, im Rundfunkbeitragsstaatsvertrag definierte personenbezogene Daten an den zentralen Beitragsservice von ARD, ZDF und Deutschlandradio übermittelt haben, hat zu keinerlei Beschwerden oder Eingaben an mich geführt.

Eingaben aus Hessen an den zentralen Beitragsservice

Im Jahr 2014 wurden 68 Anfragen und Eingaben aus dem Zuständigkeitsbereich des hr vom zentralen Beitragsservice bearbeitet, Zahlen für 2015 lagen zum Zeitpunkt meiner Berichtserstellung noch nicht vor.

Anfrage- bzw. Eingabeart	2014
Ersuchen von Rundfunkteilnehmern um Auskunft über zu ihrer Person gespeicherte Daten.	27
Fragen bezüglich der Herkunft von Daten (z. B. Adressen) bzw. der Berechtigung zur Datenerhebung.	3
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen.	24
Verlangen, Beitragszahlerdaten nicht zu anderen Zwecken zu nutzen bzw. zu übermitteln.	-
Anfragen von Finanzämtern nach Daten (insbesondere Bankverbindungen) von Beitrags-zahler(n)/innen.	1
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Beitragszahler(n)/innen.	1
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz.	12
Anzahl Vorgänge insgesamt:	**68**

Tabelle: Anfragen aus Hessen direkt an den zentralen Beitragsservice

4.2 Datenschutz bei der Creditreform Mainz

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, Brandenburg, Bremen und Hessen haben wir am 29. Oktober 2014 ergänzende Unterlagen verschickt. Eine Stellungnahme der Landesdatenschutzbeauftragten hat uns im Anschluss noch nicht erreicht.

5. Arbeitskreis der Datenschutzbeauftragten ARD/ZDF/ Deutschlandradio (AK DSB)

Die Datenschutzbeauftragten der ARD, des ZDF, des Deutschlandradios und des zentralen Beitragsservice haben sich 1979 zum Arbeitskreis Datenschutzbeauftragte ARD/ZDF (AK DSB) zusammengeschlossen, um Meinungen und Erfahrungen auszutauschen, aber auch um bei ähnlichen Problemen möglichst einheitliche Maßnahmen und Verfahren abzustimmen.

Regelmäßig trifft sich der AK DSB zweimal pro Jahr. So fanden in 2014 Tagungen in München beim Bayerischen Rundfunk und in Bonn bei der Deutschen Welle statt. In 2015 luden der Südwestrundfunk nach Karlsruhe und ARTE G.E.I.E nach Straßburg ein.

Der Vorsitz im AK DSB wechselt im Zwei-Jahres-Rhythmus. Im Berichtszeitraum hatte der Datenschutzbeauftragte des ZDF, Herr Christoph Bach den Vorsitz inne. Herr Horst Brendel, Datenschutzbeauftragter des Norddeutschen Rundfunks war zum Stellvertreter gewählt. Auf der Sitzung des AK DSB im September 2014 wurde dieses Führungsduo für weitere zwei Jahre (d.h. bis Ende 2016) im Amt bestätigt.

Im Rahmen der Sitzungen des AK DSB wurden im Berichtszeitraum insbesondere die folgenden Themen behandelt:

- Beobachtung der Entwicklungen der datenschutzrechtlichen Gesetzgebung und Rechtsprechung auf europäischer und bundesdeutscher Ebene
- Sicherstellung des Datenschutzes im redaktionellen Bereich
- Datenschutz bei hybriden Endgeräten (HbbTV)
- Auftragsdatenverarbeitung bei der Baden-Badener Pensionskasse
- Datenschutz beim Beihilfeberechnungszentrum „bbz“
- Evaluierung der Datenschutzbestimmungen im Rundfunkbeitragsstaatsvertrag
- Berichte aus dem IT-Sicherheitsgremium der ARD.

Frankfurt am Main, im Januar 2015 gez. Ulrich Göhler