WDR

23.

TÄTIGKEITS BERICHT

der Datenschutzbeauftragten

Zeitraum 1. Januar 2013 bis 31. Dezember 2014

Inhaltsverzeichnis

Vorbemerkung

Am 1. Juni 2012 wurde ich durch den Rundfunkrat des Westdeutschen Rundfunk auf Vorschlag von Intendantin Monika Piel und des Personalrats für die Dauer von vier Jahren bis zum 31. Mai 2016 zur Datenschutzbeauftragten des WDR ernannt. Ich nehme diese Aufgabe neben meiner Tätigkeit als Abteilungsleiterin für Mittelbewirtschaftung und Personalentwicklung im Hörfunk wahr.

Gemäß § 53 Abs. 7 WDR-Gesetz erstattet die Datenschutzbeauftragte des Westdeutschen Rundfunk dem Rundfunkrat alle zwei Jahre einen Bericht über ihre Tätigkeit. Der vorliegende 23. Tätigkeitsbericht dokumentiert den Zeitraum vom 1. Januar 2013 bis zum 31. Dezember 2014.

Das Thema Datenschutz hat in den vergangenen Jahren in der öffentlichen Wahrnehmung immer mehr an Bedeutung gewonnen. Die Datenschutzvorfälle in Politik und Wirtschaft werden medial und öffentlich mit starkem Interesse begleitet und diskutiert. Die zunehmende Digitalisierung aller Lebensbereiche stellt neue rechtliche, technische und organisatorische Anforderungen an Unternehmen hinsichtlich ihrer Konformität mit den Datenschutzrichtlinien.

Im 23. Tätigkeitsbericht werden allgemeine Entwicklungen des Datenschutzes sowie datenschutzrechtlich relevante Veränderungen und Problemstellungen im Westdeutschen Rundfunk während des Berichtszeitraums dargestellt.
In den Berichtszeitraum fällt u.a. das Inkrafttreten des 15. Rundfunkänderungsstaatsvertrages, mit dem der Rundfunkgebührenstaatsvertrag abgelöst wurde und die Umstellung von der Rundfunkgebühr auf den Rundfunkbeitrag erfolgte. Die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio haben das Gesetzgebungsverfahren hierzu intensiv begleitet. Gleiches gilt für die Vorbereitungsmaßnahmen der Rundfunkanstalten und des zentralen Beitragsservices von ARD, ZDF und Deutschlandradio zur Umsetzung des Rundfunkbeitragsstaatsvertrags.

Unter dem Aspekt der Gebührenlegitimation und Gebührenakzeptanz des öffentlich-rechtlichen Rundfunks bleibt ein effektiver Rundfunkteilnehmerdatenschutz auch im neuen Modell, mit dem das bisherige Gebührensystem mit seiner Anknüpfung an das Bereithalten eines Rundfunkempfangsgerätes durch den neuen geräteunabhängigen Rundfunkbeitrag abgelöst wurde, unverändert wichtig. Aufgrund der Zuständigkeit nach dem „Sitzanstaltsprinzip“ habe ich den Umstellungsprozess im Rahmen der sogenannten Controllboardsitzungen beim zentralen Beitragsservice datenschutzrechtlich intensiv und kritisch begleitet.

Ein weiterer Tätigkeitsschwerpunkt im Berichtszeitraum war die Novellierung der EU-Datenschutzrichtlinie. Nach langjährigen Verhandlungen in den verschiedenen europäischen Gremien wurde im Dezember 2015 die EU-Datenschutzgrundverordnung vom zuständigen Ausschuss gebilligt. Diese Verordnung findet auch auf den öffentlich-rechtlichen Rundfunk Anwendung.

Was den innerbetrieblichen Datenschutz im WDR angeht, gab es im Berichtszeitraum erfreulicherweise keinen Anlass für förmliche Beanstandungen, die im Verfahren nach § 53 Abs. 3 WDR-Gesetz dem Intendanten - bei gleichzeitiger Unterrichtung des Rundfunkrats - hätten mitgeteilt werden müssen.

Insgesamt ist festzustellen, dass die Themen Datenschutz und Datensicherheit sowohl faktisch durch die fortschreitende Digitalisierung in Programm, Produktion und in der Arbeitsorganisation als auch im Bewusstsein der Führungskräfte sowie der Mitarbeiterinnen und Mitarbeiter des WDR stark gestiegen sind. Ich werde in aller Regel schon präventiv in die jeweiligen Prozesse und Vorhaben eingebunden und um datenschutzrechtliche Einschätzung gebeten. Auch der Personalrat besteht bei datenschutzrechtlich relevanten Themen oder der Einführung neuer IT-Systeme stets auf ein Votum der Datenschutzbeauftragten.

Bei meiner Tätigkeit als Datenschutzbeauftragte werde ich von meinem Stellvertreter, Herrn Günter Grießbach, und Frau Petra Baumann im Sekretariat unterstützt. Beiden möchte ich an dieser Stelle für ihr kontinuierliches Engagement und die gute Zusammenarbeit ganz besonders danken.
Ebenfalls danken möchte ich dem IT- Sicherheitsbeauftragten des WDR, Herrn Norbert Gust, dem Kollegen Roland Boysen im Justiziariat, Frau Sandra Schlechtriem sowie der Datenschutzbeauftragten des zentralen Beitragsservice, Frau Kerstin Arens und ihrem Kollegen Christian Kruse für die stets kompetente, engagierte und kollegiale Zusammenarbeit.

Köln, im Februar 2016 Beate Ritter

A. Aufgaben der Datenschutz-beauftragten

Nach § 53 Abs. 1 WDR-Gesetz tritt der/die Beauftragte für den Datenschutz beim WDR an die Stelle des oder der Landesbeauftragten für den Datenschutz und Informationsfreiheit, soweit es um datenschutzrechtliche Fragen geht. Die Beauftragte für den Datenschutz beim WDR nimmt ausdrücklich nicht die Aufgaben einer Beauftragten für die Informationsfreiheit wahr.

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

Den Schwerpunkt meiner Arbeit bildet die datenschutzrechtliche Beurteilung von Prozessen und Projekten sowie die Beratung sämtlicher Bereiche des Hauses einschließlich des Beitragsservices. Bei festgestellten Mängeln und Defiziten bestand in den betroffenen Abteilungen und Direktionen Bereitschaft zur Abhilfe. Meine Verbesserungsvorschläge wurden aufgenommen. Im Berichtszeitraum habe ich außerdem eine datenschutzrechtliche Prüfung bei der vom WDR mit der Beihilfeabwicklung beauftragten Rheinischen Versorgungskasse durchgeführt.

Festzustellen ist, dass die Digitalisierung beim WDR mehr denn je und in allen Bereichen voranschreitet. Hierbei ist erkennbar, dass zunehmend die Einbindung der Datenschutzbeauftragten im Rahmen laufender Projekte oder Prozesse oder aber auch aufgrund entsprechender Nachfragen seitens der Fachbereiche des Hauses oder des Personalrates in erfreulichem Maße sichergestellt und quantitativ erheblich angestiegen ist.

Dementsprechend bin ich verstärkt auch beim Abschluss von Verträgen, soweit die Federführung beim WDR liegt auch bei ARD-Verträgen, bereits im Rahmen der Ausschreibung beteiligt worden und konnte die datenschutzrechtlichen Anforderungen z.B. an Medienforschungsverträge, Vergabesoftware oder Streamingverträge mitgestalten.

Die Informationen, die ich als Bürgerservice und als Hilfestellung auch in das Internetangebot des WDR eingestellt habe, sind dort weiterhin abrufbar. Auch das Intranetangebot der Datenschutzbeauftragten des WDR steht weiterhin für die Mitarbeiter/innen bereit und wird regelmäßig angepasst.

Nach § 11 Abs. 1 WDR-Gesetz hat jeder das Recht, sich unmittelbar an die Datenschutzbeauftragte des WDR zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den WDR in seinen schutzwürdigen Belangen verletzt worden zu sein. In erster Linie machen hiervon Rundfunkteilnehmer/innen und auch Mitarbeiter/innen Gebrauch, die sich wie andere Bürger schriftlich, telefonisch oder per E-Mail an mich wenden. Es geht dabei nicht nur um datenschutzrechtliche Beschwerden. Vielfach werde ich auch um Auskünfte im Zusammenhang mit dem Beitragseinzug oder der Behandlung von Teilnehmerpost gebeten. Sofern es sich hierbei um Fragen zum individuellen Teilnehmerkonto handelt, leite ich diese an die Datenschutzbeauftragte des zentralen Beitragsservice, Frau Kerstin Arens, weiter. Sie veranlasst eine qualifizierte Beantwortung des Auskunftsersuchens und gibt mir diese zur Kenntnis.

B. Entwicklung des Datenschutzrechts

1. Europa

1.1. EU-Datenschutzgrundverordnung

Im Berichtszeitraum galt noch die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (EU-Datenschutzrichtlinie), die aus dem Jahr 1995 stammt. Sie zielt darauf ab, die Hindernisse für den freien Datenverkehr aus dem Weg zu räumen, ohne den Schutz von personenbezogenen Daten zu beeinträchtigen. Aufgrund dieser Richtlinie sollen die personenbezogenen Daten der EU-Bürger in der gesamten Europäischen Union einen gleichwertigen Schutz genießen. Allerdings war die Richtlinie aufgrund der äußerst unterschiedlichen nationalen datenschutzrechtlichen Regelungen in den Mitgliedsländern sowie aufgrund der aktuellen technischen Entwicklungen und der damit verbundenen neuen Gefahren für den Datenschutz überarbeitungsbedürftig.

Das Rechtssetzungsverfahren auf europäischer Ebene zur Datenschutzgrundverordnung hat mehrere Jahre in Anspruch genommen. Auch ARD, ZDF und die EBU haben sich mit ihren Positionen zu den spezifischen rechtlichen Anforderungen an den Datenschutz und seine Aufsicht in den (öffentlich-rechtlichen) Medien in das Verfahren eingebracht. Im Dezember 2015 hat der zuständige Ausschuss nun einen mit dem Rat vereinbarten Kompromiss zur europäischen Datenschutzgrundverordnung gebilligt, mit der der Flickenteppich datenschutzrechtlicher Regelungen in den 28 Mitgliedstaaten abgelöst und europaweit eine einheitliche Grundlage geschaffen, wird, die für den gesamten privaten und öffentlichen Bereich gilt.

Die neue EU-Datenschutz-Grundverordnung umfasst auch den Datenschutz im Medienbereich, so dass die Rundfunkanstalten unmittelbar von der Neuregelung betroffen sein werden.

Die wichtigsten Punkte der Neuordnung sind:

Verarbeitung der Daten nur nach ausdrücklicher Einwilligung: Der Nutzer soll Herr seiner Daten werden. Er soll seine Einwilligung auch leicht wieder zurückziehen können.

Kinder und soziale Medien: Kinder unter einem bestimmten Alter benötigen die Zustimmung der Eltern, um ein Social-Media-Konto zu eröffnen, wie zum Beispiel bei Facebook, Instagram oder Snapchat. Dies ist bereits in den meisten EU-Ländern üblich. Die neuen, flexiblen Vorschriften räumen den Mitgliedstaaten einen Spielraum für die Altersgrenzen ein (allerdings muss diese mindestens bei 13 und höchstens bei 16 Jahren liegen).

Recht auf Vergessenwerden: Die Verbraucher sollten ihre Einwilligung geben müssen, aber genauso einfach sollten sie sie auch wieder zurückziehen können. Sie bekommen ein "Recht auf Vergessenwerden", d.h. ein Recht darauf, dass auf ihren Wunsch ihre persönlichen Daten aus den Speichern von Unternehmen auch wieder gelöscht werden müssen.

Datenlecks oder "gehackte" Daten: Bei Verstößen gegen den Schutz personenbezogener Daten müssen die Anbieter die zuständigen Behörden so schnell wie möglich informieren, so dass die Nutzer geeignete Maßnahmen ergreifen können.

Verständliche Sprache: Mit den neuen Vorschriften soll die Praxis des "Kleingedruckten" abschafft werden. Die Verbraucher sollen in klarer, verständlicher Sprache und mit leicht verständlichen Symbolen informiert werden, bevor die Daten gespeichert werden.

Strafen: Wenn Firmen gegen die Regeln verstoßen, drohen ihnen Strafen von bis zu vier Prozent des Jahresumsatzes.

Unternehmen müssen Datenschutzbeauftragte anstellen: Unternehmen müssen eine/n Datenschutzbeauftragte/n benennen, wenn sie im großen Ausmaß sensible Daten verarbeiten oder das Verhalten vieler Verbraucher überwachen.

Zentrale Anlaufstellen für Beschwerden und die Durchsetzung der neuen Regeln: Die nationalen Datenschutzbehörden werden ausgebaut und sollen zu zentralen Anlaufstellen für Bürger werden, wo sie ihre Beschwerden über Verstöße gegen die Datenschutzvorschriften einreichen können. Die Zusammenarbeit zwischen diesen nationalen Behörden soll erheblich verstärkt werden, um einen einheitlichen Schutz der personenbezogenen Daten innerhalb der Union sicherzustellen.

Für Medienunternehmen wie den WDR ist insbesondere Art. 80 der EU-Datenschutz-Grundverordnung von Interesse. Nach dem ersten Entwurf konnten die Mitgliedsstaaten „für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen oder Ausnahmen“ vorsehen. In der durch den sog. LIBE-Ausschuss des Europäischen Parlaments nun gebilligten Endfassung wird den Mitgliedsstaaten nun durch die EU-Datenschutzgrundverordnung vorgegeben, „das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen“. Für die öffentlich-rechtlichen Rundfunkanstalten gilt zudem, dass auch nach dem Protokoll zum Amsterdamer Vertrag 1997 die nationale Gesetzgebungskompetenz und damit in der Bundesrepublik die des Landesgesetzgebers für den Rundfunk besteht. Damit ist die von Seiten der öffentlich-rechtlichen Rundfunkanstalten vertretene Regelungsvariante im Verordnungstext aufgegriffen worden.

Über den Verordnungstext stimmt das Plenum des Europäischen Parlaments im Frühjahr 2016 ab. Nach dem Inkrafttreten haben die Mitgliedstaaten zwei Jahre Zeit, die neuen Vorschriften umzusetzen.

Im Rahmen des nationalen Umsetzungsverfahrens werden meine Kolleginnen und Kollegen in der ARD, dem ZDF und Deutschlandradio im Sinne der öffentlich-rechtlichen Rundfunkanstalten darauf zu achten haben, dass die datenschutzrechtlichen Besonderheiten der Rundfunk- und Pressefreiheit wie auch die Stellung der Rundfunkdatenschutzbeauftragten nicht in Frage gestellt wird und es weiterhin bei einer staatsfernen Ausgestaltung auch der datenschutzrechtlichen Aufsichtsbehörden für den öffentlich-rechtlichen Rundfunk bleibt.

Über den Fortgang des Umsetzungsprozesses und die Implementierung auf nationaler Ebene bzw. Landesebene wird ausführlich im kommenden Tätigkeitsbericht für die Jahre 2015 und 2016 zu berichten sein.

1.2. Urteile

Entscheidung des Europäischen Gerichtshofs für Menschenrechte zur Vorratsdatenspeicherung

Die EU-Richtlinie zur Vorratsdatenspeicherung, die eine anlasslose Vorratsspeicherung von Verkehrs- und Bestandsdaten für mindestens 6 Monate vorsah, verstieß gegen europäisches Recht und ist ungültig. Das hat der Europäische Gerichtshof (EuGH) mit Urteil vom 8. April 2014 entschieden. Das Gericht erteilte der undifferenzierten und automatischen Erfassung von Verkehrsdaten in der Telekommunikation eine Absage. Zwar werde der Wesensgehalt der Achtung der Privatsphäre (Art. 7 der Europäischen Grundrechtscharta), des Schutzes personenbezogener Daten (Art. 8) und der Meinungsfreiheit (Art. 11) durch die Vorratsdatenspeicherung nach Ansicht des EuGH nicht angetastet, solange sie den Inhalt der elektronischen Kommunikation nicht zur Kenntnis gibt, die Grundsätze des Datenschutzes und der Datensicherheit eingehalten sowie die Inhalte von Nachrichten der mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen nicht offen gelegt werden. Die Vorratsdatenspeicherung, wie sie der EuGH zu beurteilen hatte, sei allerdings ein Eingriff in die genannten Grundrechte, der als besonders schwerwiegend anzusehen sei. Dieser Eingriff müsse, um rechtmäßig zu sein, nicht nur geeignet sein, die verfolgte Zielsetzung zu erreichen. Er müsse auch erforderlich und verhältnismäßig sein, dürfe also die Grenzen dessen nicht überschreiten, was zur Erreichung des Ziels geeignet und erforderlich sei. Die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, sei zwar von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit und deren Wirksamkeit könne in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen. Diese dem Gemeinwohl dienende Zielsetzung könne die Speicherungsmaßnahme für die Kriminalitätsbekämpfung für sich genommen aber nicht rechtfertigen, soweit die Speicherung auf Vorrat, also anlasslos und ohne jede Differenzierung, vorgenommen wird.

Der EuGH fordert, dass für Personen, deren Kommunikationswege nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen, Ausnahmen vorzusehen seien. Zu den Berufsgeheimnisträgern in diesem Sinne gehören auch die Journalistinnen und Journalisten.

In Deutschland hat sich die Rechtslage durch das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“, das am 18. Dezember 2015 in Kraft getreten ist, geändert. Näheres dazu unter B 2.1.

EuGH Urteil zum sog. Recht auf Vergessen

Der Suchmaschinenbetreiber Google kann dazu verpflichtet werden, Verweise auf Webseiten mit sensiblen persönlichen Daten aus seiner Ergebnisliste zu streichen. Das entschied der Europäische Gerichtshof in Luxemburg in einem Urteil vom 13. Mai 2014 (Rs.C-131/12) unter Verweis auf die EU-Datenschutzrichtlinie. Danach muss Google künftig auf Antrag des Betroffenen veraltete oder irrelevante Informationen löschen. Nach Ansicht des Gerichts ist der Suchmaschinenbetreiber für die Verarbeitung der Daten verantwortlich. Ein Betroffener könne sich mit der Bitte um Änderung der Suchergebnisse direkt an Google wenden. Dies

gelte, wenn die Person nachweise, dass sich Links auf veraltete oder irrelevante Informationen bezögen.
In diesem Zusammenhang hat der Gerichtshof betont, dass durch das Betreiben von Suchmaschinen eine zusätzliche Gefährdung der Grundrechte auf Achtung des Privatlebens und zum Schutz personenbezogener Daten geschaffen wird, indem es jedem Internetnutzer allein durch die Eingabe eines Namens die Möglichkeit verschafft, mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen zu erhalten.
Darin können zahlreiche Aspekte aus dem Berufs- oder Privatleben enthalten sein, die ohne die betreffende Suchmaschine nicht oder nur sehr schwer miteinander verknüpft werden können und die es erlauben, ein mehr oder weniger detailliertes Profil der Person zu erstellen. Wegen seiner potentiellen·Schwere könne ein solcher Eingriff nicht allein mit den wirtschaftlichen Interessen des Betreibers einer Suchmaschine begründet werden. Allerdings sei zu berücksichtigen, dass mit der Entfernung von Links auch berechtigte Interessen von Menschen betroffen sind, die sich Zugang zu den Informationen verschaffen möchten. Aus diesem Grund sei in jedem Einzelfall eine Abwägung vorzunehmen mit dem Ziel, einen angemessenen Ausgleich unter den berührten Grundrechten herbeizuführen.

Das Urteil des EuGH ist auch für die Rundfunkanstalten von Bedeutung. Denn der Gerichtshof konstatiert in den Entscheidungsgründen, dass aufgrund des datenschutzrechtlichen Medienprivilegs die Medien selbst zur Löschung nicht verpflichtet sind. Dieses Privileg stehe – so das Gericht – den Suchmaschinenbetreibern nicht zu.
Kurz nach dem Erlass des Urteils hat Google einen sog. Löschbeirat einberufen, damit dieser Regeln und Empfehlungen zum Vorgehen bei komplizierten Löschanträgen ausarbeitet. Das Gremium, dem auch die frühere Bundesjustizministerin Frau Dr. Sabine Leutheusser-Schnarrenberger angehört, konsultierte dazu in zahlreichen europäischen Ländern Sachverständige und diskutiert auch mit der Öffentlichkeit die Folgen des Urteils. Der Löschbeirat hat Google empfohlen, mehr Anträge zum Recht auf Vergessen als bislang zu bewilligen. Uneinig sind sich die Experten offenbar über die Reichweite des Löschungsanspruchs. Mehrheitlich plädieren sie dafür, dass bei einem Anspruch auf das Löschen von Links nur die Links auf EU-Domains gelöscht werden, wie es seit dem Luxemburger Gerichtsurteil schon Praxis bei Google ist. Demgegenüber fordert Frau Dr. Leutheusser-Schnarrenberger eine globale Löschung für alle Domains. Im Streit über ein weltweites Recht auf Vergessen (werden) im Internet stellt sich Google nun gegen eine Anordnung aus Frankreich. Google erklärte, die Pariser Datenschutz-Aufsicht sei bei der Löschung von Suchergebnissen nicht global zuständig. Der weitere Fortgang dieser Angelegenheit bleibt spannend.

Save Harbor - Patriot Act

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. Mit Blick auf den sog. Patriot Act könne nicht sichergestellt werden, dass Daten durch das Safe-Harbor-Abkommen wirksam vor dem Zugriff US-Amerikanischer Sicherheitsbehörden geschützt seien.

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 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.

Am 2. Februar 2016 haben die EU und die USA sich auf ein neues Datenschutzabkommen geeinigt. Aus datenschutzrechtlicher Sicht wird das Abkommen jedoch den Anforderungen, die der EuGH in seiner Entscheidung im Oktober 2015 formuliert hat, nicht gerecht. Über vage Absichtserklärungen geht das Abkommen nicht hinaus.

2. Bundesrecht

2.1. Vorratsdatenspeicherung

Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

In Deutschland war die Vorratsdatenspeicherung per Gesetz auf Basis der EU-Richtlinie im Jahr 2007 eingeführt worden. Mit Urteil vom 2. März 2010 hatte das Bundesverfassungsgericht dieses Gesetz für verfassungswidrig und nichtig 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.

Mit dem Urteil des EuGH zur Rechtswidrigkeit der anlasslosen Vorratsdatenspeicherung vom 8. April 2014 (siehe oben B 1.2) und dem damit verbundenen Wegfall der europarechtlichen Grundlage war auch die Bundesregierung zunächst von ihrem Vorhaben abgerückt, schnell ein neues Gesetz zur Vorratsdatenspeicherung zu erlassen.

Vor dem Hintergrund zahlreicher terroristischer Anschläge in Europa hat der Bundestag dann doch am 27. Mai 2015 einen neuen Gesetzesentwurf vorgelegt, dem erneut eine anlasslose Vorratsdatenspeicherung zugrunde lag. 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.

ARD, BDZV, DJV, Deutscher Presserat, VDZ, dju in Verdi, VPRT und ZDF (BT-Drs. 18/5171; BT-Drs. 18/5088) haben dazu eine gemeinsame Stellungnahme vorgelegt und kritisiert, dass die anlasslose Vorratsdatenspeicherung die Presse- und Rundfunkfreiheit beeinträchtige. Vor allem werde dadurch der Informantenschutz und das Redaktionsgeheimnis geschwächt. Auch die Datenschutzbeauftragten von ARD und ZDF haben an dieser Stellungnahme mitgewirkt. Bedauerlicherweise hat diese Kritik in der Beschlussfassung durch den Bundestag am 16. Oktober 2015 keine Berücksichtigung gefunden. Das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ ist am 18. Dezember 2015 in Kraft getreten. Beim Bundesverfassungsgericht liegen inzwischen bereits Klagen gegen das Gesetz vor.

2.2. Beschäftigtendatenschutz

Das Beschäftigtendatenschutzgesetz hat auch im Berichtszeitraum und bis heute keine relevanten Veränderungen erfahren, so dass für die Beschäftigten des WDR weiterhin § 29 Landesdatenschutzgesetz NRW zur Datenverarbeitung bei Dienst- und Arbeitsverhältnissen gilt.

2.3. 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 Datennetze 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.

2.4. Gesetzentwurf der Bundesregierung zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf verabschiedet, mit dem die bisherige

organisatorische Anbindung der/des Bundesbeauftragten für den Datenschutz an das Bundesinnenministerium gestrichen und durch die Errichtung einer neuen obersten Bundesbehörde ersetzt werden soll. Die/der Bundesbeauftragte für den Datenschutz soll der ausschließlichen parlamentarischen und gerichtlichen Kontrolle unterstellt und die bisherige Rechtsaufsicht durch die Bundesregierung und die Dienstaufsicht durch den Bundesinnenminister ersatzlos gestrichen werden. Mit dieser Änderung wird die Rechtsstellung der/des Bundesbeauftragten für den Datenschutz den Anforderungen gerecht, die der Europäische Gerichtshof in seiner Entscheidung von 9. März 2011 für die Unabhängigkeit der Aufsichtsbehörden von jeglicher staatlicher Einflussnahme formuliert hat. Das Gesetz wurde am 18. Dezember 2014 vom Bundestag verabschiedet.

3. Länder- bzw. Landesrecht

3.1. Beitragsmodell - 15. Rundfunkänderungsstaatsvertrag

Mit dem 15. Rundfunkänderungsstaatsvertrag wurde die Finanzierung des öffentlich-rechtlichen Rundfunks neu geordnet. Ab dem 1. Januar 2013 wurde die geräteabhängige Rundfunkgebühr durch ein geräteunabhängiges Rundfunkbeitragsmodell ersetzt. Wie bereits im 22. Tätigkeitsbericht ausgeführt, haben sich die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio mit ihren datenschutzrechtlichen Anforderungen in das Gesetzgebungsverfahren eingebracht. Den wichtigsten Punkten wurde im Gesetzestext Rechnung getragen. Auch die Umsetzung haben die Rundfunkdatenschutzbeauftragten in ihrer Funktion als datenschutzrechtliche Aufsichtsbehörden intensiv und kritisch begleitet. Dies geschah insbesondere im Rahmen der regelmäßigen Controllboardsitzungen beim zentralen Beitragsservice, an denen ich als Datenschutzbeauftragte des WDR federführend für die ARD teilnahm.

Was die Inhalte der Neuregelungen angeht, sind diese zum Teil durchaus datenschutzfreundlicher gestaltet als die Vorgängerregelungen. Insbesondere konnten die früheren Nachforschungen bei den Bürgerinnen und Bürgern zum Bereithalten von Rundfunkgeräten entfallen. Auch elementare datenschutzrechtliche Vorgaben wie die vorrangige Direkterhebung von Daten beim Betroffenen bleiben gewahrt.

In der Kritik stand allerdings der einmalige Meldedatenabgleich mit den Meldebehörden nach § 14 Abs. 9 Rundfunkbeitragsstaatsvertrag zum Zwecke der Bestands- und Ersterfassung von Beitragsschuldnern. Der Gesetzgeber hat in § 14 Abs. 8 des Rundfunkbeitragsstaatsvertrages festgelegt, dass die gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnung einschließlich aller Angaben zur Lage der Wohnung zu übermitteln sind. Für die möglichst vollständige Erfassung aller Beitragsschuldner im Sinne einer größeren Beitragsgerechtigkeit ist es erforderlich, dass Beitragsschuldner nicht nur einer bestimmten Adresse sondern auch einer konkreten Wohnung zugeordnet werden können (vgl. auch §§ 2 Abs. 1, 3 Abs. 1 Rundfunkbeitragsstaatsvertrag).

Der Bayerische Verfassungsgerichtshof hat den einmaligen Meldedatenabgleich mit seiner Entscheidung vom 18. April 2013 dahingehend beurteilt, dass es sich hierbei um ein effizientes Kontrollinstrument handele, mit dem in der Umstellungsphase eine verlässliche und möglichst vollständige Erfassung der Rundfunkbeitragsschuldner im privaten Bereich in einem überschaubaren Zeitraum sichergestellt werden soll. Der einmalige Meldedatenabgleich diene der Vermeidung von Vollzugsdefiziten und einer größeren Beitragsgerechtigkeit. Hiergegen haben die Nachteile für die Betroffenen laut Bayerischem Verfassungsgerichtshof zurückzutreten. Das Interesse, beitragsrelevante Sachverhalte nicht zu offenbaren und nicht als Beitragsschuldner identifiziert zu werden, sei unbeachtlich. Nach der Entscheidung haben die Nachteile, die mit der Datenübermittlung und -verarbeitung ohne Kenntnis und Einwilligung der Betroffenen verbunden sind, auch für diejenigen Personen, die später nicht als Beitragsschuldner herangezogen werden, eher geringes Gewicht. In der Entscheidung wird außerdem betont, dass die von den Meldebehörden übermittelten Daten bei der Landesrundfunkanstalt durch eine strikte Zweckbindung und strenge Löschungspflichten abgesichert sind.

Neben dieser Entscheidung des Bayerischer Verfassungsgerichtshof vom 18. April 2013 sind noch zahlreiche andere Entscheidungen zur Rechtmäßigkeit des einmaligen Meldedatenabgleichs ergangen, so u.a.:

- VG Berlin, Beschl. v. 22.05.2013
- VG Leipzig Beschl. v. 15.07.2013
- OVG Berlin-Brandenburg (Beschl. v. 06.08.2013 OVG 11 S 23.13)
- OVG Niedersachsen, Beschl. v. 10.09.2013 4 ME 204/13

Im Rahmen der Evaluierung des Rundfunkbeitrags und der Beratungen zum 16. Rundfunkänderungsstaatsvertrag ist ein erneuter Meldedatenabgleich im Gespräch. Auch hierzu hat sich der Arbeitskreis der Rundfunkdatenschutzbeauftragten von ARD, ZDF und Deutschlandradio bereits positioniert (vgl. unten D 1).

3.2. Novellierung WDR-Gesetz

Die Novellierung des WDR-Gesetzes wurde am 27. Januar 2016 im Landtag NRW beschlossen. Die Änderung tritt am Tag nach der Verkündung in Kraft. Datenschutzrechtlich gibt es zwei markante Änderungen:

1. Eine Erweiterung des Medienprivilegs in § 49 Abs. 3 Satz 2 WDR-Gesetz analog zur Regelung beim ZDF um den Passus:

   „oder durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde."

2. Die Hauptamtlichkeit des/der Datenschutzbeauftragten des WDR in § 53 Abs. 2 Satz 2 WDR-Gesetz statt der bisher möglichen Nebenamtlichkeit:

   „Sie oder er darf während dieser Tätigkeit keine weiteren Aufgaben innerhalb der Anstalt übernehmen."

Die gesetzgeberische Stärkung des Medienprivilegs ist auch aus datenschutzrechtlicher Sicht zu begrüßen, ist das Medienprivileg doch fundamentaler Bestandteil der Rundfunkfreiheit. Auch die Neuregelung zur künftigen Hauptamtlichkeit des/der Datenschutzbeauftragten des WDR kann ich insoweit gut nachvollziehen als hiermit vom Gesetzgeber eine weitere Stärkung der Unabhängigkeit des Amts und der damit verbundenen Aufsichtsfunktion verbunden ist. Mit Blick auf die Staatsferne des öffentlich-rechtlichen Rundfunks ist die Unabhängigkeit des/der Rundfunkdatenschutzbeauftragten ein hohes Gut, das es – auch im Rahmen des künftigen nationalen Umsetzungsverfahrens zur EU-Datenschutzgrundverordnung – zu schützen und zu bewahren gilt.

C. Datenschutz im WDR

1. Allgemeines

Im Datenschutzreferat haben die Anfragen aus den unterschiedlichen Bereichen des Hauses erheblich zugenommen. Der Datenschutz hat insgesamt in Gesellschaft, Politik und Medien an Bedeutung und Interesse gewonnen. Dies ist sicher u.a. auf die Abhörskandale zurück zu führen, durch die das Bewusstsein für den Missbrauch von Daten allgemein in der Bevölkerung deutlich gestiegen ist. Auch in der Berichterstattung des WDR wurde und wird diese Thematik immer wieder aus unterschiedlichsten Blickwinkeln beleuchtet. Besonders erwähnenswert ist in diesem Zusammenhang die WDR-Reportage „Das Wunder von Brüssel" von WDR-Korrespondent Christian Feld, in dem der lange und schwierige Rechtsetzungsprozess zur EU-Datenschutzgrundverordnung beleuchtet wird. Bemerkenswert ist auch, dass Datenschutz und Datenklau Thema des höchst erfolgreichen multimedialen Projekts „Supernerds – ein Überwachungsabend" war, in dem WDR und „Schauspiel Köln" gemeinsam im Rahmen eines innovativen und interaktiven Formats geheime Datenströme für das Publikum sichtbar gemacht haben. Im Vorfeld der Programmaktion hat die Redaktion auch die Beratung und Abstimmung mit und durch das Datenschutzreferat in Anspruch genommen.

Die Themen und Anfragen, die mich als Datenschutzbeauftragte des WDR erreichen, sind aber sehr viel breiter gefächert. Sie reichen von der Einsichtnahme in groupwise–accounts z.B. bei unabsehbaren Abwesenheiten von Mitarbeitern, über die Mitwirkung bei Leistungsverzeichnissen, Änderung oder Einführung datenschutzrechtlicher Vorschriften, Prüfung der Einführung von IT- Systemen bis hin zur Prüfung von Einrichtungen und Unternehmen, die vom WDR mit der Verarbeitung von Daten beauftragt sind.

Im Folgenden werden nur einige Prüfungen und Befassungen beispielhaft dargestellt. Dem Thema Beitragseinzug ist danach ein gesondertes Kapitel gewidmet.

2. Datenschutz im Personalbereich

2.1. Mitarbeiterbefragung

Im September 2013 wurde zum dritten Mal eine Mitarbeiter/innenbefragung im WDR durchgeführt. Erstmalig fand die Erhebung als Onlinebefragung statt.
Hierzu wurde das Befragungstool der Firma Questback eingesetzt. Als Datenschutzbeauftragte wurde ich im Vorfeld um Prüfung und Beratung gebeten. Dabei galt vor allem sicherzustellen, dass

- die zugesagte Anonymität sowohl bei der Befragung als auch bei der Auswertung gewahrt wurde,
- dass keine unbefugten Dritten die Datensätze mit den Antworten der Mitarbeiter/innen zur Kenntnis erhielten,
- die beauftragte Firma im Rahmen der Auftragsdatenvereinbarung die notwendigen technischen und organisatorischen Voraussetzungen und Maßnahmen erfüllt
- die Daten unverzüglich gelöscht werden nachdem der Zweck der Datenerhebung- und verarbeitung beendet bzw. entfallen war
- die externe Firma im Rahmen der Auftragsdatenverarbeitung für den WDR sich der Kontrolle der Datenschutzbeauftragten des WDR unterwirft.

Im Rahmen der datenschutzrechtlichen Beratung haben wir gemeinsam mit der HA KomForS/ Medienforschung, die für die Durchführung und Auswertung der Mitarbeiterbefragung zuständig war, die Realisierung der o.g. Punkte erreichen können. Nachfragen aus der Mitarbeiterschaft etwa zur Gewährleistung der Anonymität der Befragung konnten somit zur Zufriedenheit beantwortet werden.

2.2. Antrag auf Videoüberwachung anlässlich wiederkehrender Getränkeverunreinigungen

Mitte Oktober 2013 hat ein Produktionsmitarbeiter bei Phoenix festgestellt, dass sich in seiner Wasserflasche, die er wie seine Kollegen regelmäßig in einem Lagerraum abstellte, eine fremde Substanz befand. Nachdem dies mehrfach geschah, hat der zustände Vorgesetzte den TÜV Rheinland um eine Analyse des verunreinigten Wassers gebeten. Es stellte sich heraus, dass dem Wasser Spülmittel/Duschgel beigemengt worden war. Dies kann bei Verzehr zu erheblicher Übelkeit und Magenverstimmung führen. Daraufhin wurde die Polizei durch Aufgabe einer Anzeige gegen unbekannt eingeschaltet, die aber ohne konkreten Tatverdächtigen keine Ermittlungen aufnahm. Daraufhin wurden mein Kollege Bach vom ZDF und ich gebeten zu prüfen, ob hier eine verdeckte Videoüberwachung möglich sei. Nachdem hauptsächlich WDR-Mitarbeiter von der Gefahr der weiteren Getränkeverunreinigung und somit gesundheitlicher Schäden betroffen waren, habe ich die Prüfung federführend übernommen. Nach eingehender Prüfung des Sachverhalts bin ich zum Ergebnis gelangt, dass eine verdeckte Videoüberwachung im vorliegenden Fall **nicht** die ultima ratio darstellt.

Nach der Rechtsprechung des Bundesarbeitsgerichts ist eine verdeckte Videoüberwachung durch den Arbeitgeber zulässig, wenn:

- der **konkrete Verdacht einer strafbaren Handlung** oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht
- **weniger einschneidende Mittel** zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit praktisch das einzige verbleibende Mittel darstellt und
- sie insgesamt **nicht unverhältnismäßig** ist.

Der konkrete Verdacht einer strafbaren Handlung (Körperverletzung) lag im konkreten Fall vor. Im Rahmen der arbeitgeberseitigen Fürsorgepflicht hatte Phoenix bzw. der WDR als Arbeitgeber aber vor allem dafür Sorge zu tragen, dass von den Arbeitsbedingungen keine Gefahr für Leib und Leben der Mitarbeiter ausgeht. Es ging somit für den WDR als Arbeitgeber in erster Linie um die **Gefahrenabwehr** und den Schutz der Kolleginnen und Kollegen bei Phoenix gegen weitere Verunreinigungen ihrer Getränke.

Auf meine Empfehlung hat der zuständige Abteilungsleiter daraufhin eine außerordentliche Bereichsversammlung mit seinen Mitarbeitern abgehalten. Durch die Information der betroffenen Kollegen und ein entsprechendes Informationsschreiben des Vorgesetzten waren die Mitarbeiter nun angehalten, ihre Getränke stets vor Verzehr auf Auffälligkeiten zu überprüfen.

Da der Lagerraum, in dem die Verunreinigungen stattfanden, aber auch für andere Kollegen, Freie und gelegentliche externe Gäste zugänglich ist, war jedoch nicht auszuschließen, dass der Gefahrenabwehr mit der Bereichsversammlung und dem Informationsschreiben nicht vollumfänglich Genüge getan war. Die Rechtsprechung fordert allerdings bei einer verdeckten Videoüberwachung die Verhältnismäßigkeit zwischen dem Eingriff in die Persönlichkeitsrechte der per Video Aufgenommenen und den schutzwürdigen Interessen des

Arbeitgebers (hier: Gefahrenabwehr und – bei internem Täter - Ergreifen arbeitsrechtlicher Konsequenzen).

Hierbei galt es im konkreten Fall zu berücksichtigen, dass der Durchgangsraum/das Lager, in dem ggfs. eine verdeckte Videoüberwachung stattfinden würde, von einer nicht unerheblichen Zahl festangestellter und freier Mitarbeiter benutzt. Somit beträfe der Kreis, der „unverschuldet“ heimlich Aufgenommen nicht nur die festen Produktionsmitarbeiter sondern auch die Freien sowie andere Kollegen und ggfs. auch externe Gäste, die sich gelegentlich dort aufhalten. Der datenschutzrechtlich als erheblich einzustufende Eingriff bei einer verdeckten Videoüberwachung hätte somit eine Vielzahl von Personen betroffen. Hinzu kommt, dass die verdeckte Videoüberwachung nur als ultima ratio zum Einsatz kommen soll; also als letztes Mittel, das zur Erreichung der vollumfänglichen Gefahrenabwehr zur Verfügung steht.

Da hier eine offene Videoüberwachung als milderes und gleichzeitig abschreckendes Mittel zur Verfügung stand, habe ich in Abstimmung mit meinem ZDF-Kollegen diese als datenschutzrechtlich verhältnismäßige Maßnahme befürwortet. Gleichzeitig habe ich darum gebeten, dass der Kreis der Zugriffsberechtigten auf die Videodaten streng eingegrenzt und die offene Videoüberwachung zeitlich befristet werden sollte. Dem wurde Rechnung getragen. Ebenso der Vorgabe, dass die Videoaufnahmen umgehend gelöscht werden sobald eine zeitnahe Sichtung erfolgt ist und diese keine Feststellung zu weiteren Verunreinigungen ergeben hat oder ein Täter durch die Videoaufnahmen festgestellt werden konnte.

2.3. Prüfung Rheinische Versorgungskasse/ Bearbeitung Beihilfeanträge

Die Rheinische Versorgungskasse (RVK) ist eine selbstständige Körperschaft des öffentlichen Rechts mit eigener Satzung und Budgetverantwortung.
Die Geschäftsführung obliegt nach dem Versorgungs- und Zusatzversorgungskassengesetz dem Landschaftsverband Rheinland (LVR).

Die RVK ist vom WDR mit der Bearbeitung der Beihilfen beauftragt. Sinn und Zweck des vom Datenschutzreferat bei der RVK durchgeführten Audits war die Prüfung, ob und inwieweit die LVR die ihr im Rahmen der Beihilfebearbeitung übersandten personenbezogenen und sensiblen Mitarbeiterdaten im Rahmen der gesetzlichen Vorgaben des §11 LDSG NRW für die Auftragsdatenverarbeitung datenschutzkonform speichert und verarbeitet.

Am 28. November 2014 habe ich der RVK im Rahmen des Audits einen Besuch abgestattet, in dem die zuständigen Abteilungs-/Gruppenleiter/innen der RVK sowie der Datenschutzbeauftragte der RVK für Nachfragen zu den zuvor schriftlich übersandten Unterlagen zur Verfügung standen. Auch wurde mir und meinem Mitarbeiter, Herrn Grießbach, eine Einsichtnahme in die Bearbeitungssysteme im Rahmen des datenschutzrechtlich Möglichen gewährt. Der Besuch fand im Gebäude der RVK statt. In der Folge gab es darüber hinaus eine Begehung des Rechenzentrums der RVK in Köln Deutz unter Beteiligung des IT- Sicherheitsbeauftragten des WDR.

Im Vorfeld hatte die RVK bereits auf den von uns übersandten ausführlichen Fragenkatalog geantwortet. Die Fragen wurden an die Geschäftsleitung und den IT-Sicherheits- und Datenschutzbeauftragten der RVK gestellt und von diesen vollumfänglich beantwortet.

Bei der eingehenden Prüfung konnten wir feststellen, dass es für die verschiedenen Geschäftsbereiche der RVK streng zweck- und kundenbezogene Berechtigungskonzepte gibt. Die Art der Speicherung sowie die Zugriffs- und Bearbeitungsrechte der für die WDR-Beihilfeanträge zuständigen Mitarbeiter und Administratoren sind datenschutzkonform ausgestaltet und beschränkt auf einen festgelegten Personenkreis, der auch datenschutzrechtlich im Umgang mit sensiblen Daten geschult ist. Die Datenleitung zwischen RVK und WDR ist gesichert und verschlüsselt. Das IT- Sicherheitskonzept entspricht hohen datenschutzrechtlichen Anforderungen. Auch was das Management der Datensicherung sowie die Zutritts- und Sicherheitsvorkehrungen des Rechenzentrums angeht, konnten wir uns von der Datenschutzkonformität überzeugen.

Insgesamt hat die Prüfung ergeben, dass die RVK mit großer Sensibilität und hohen Sicherheitsstandard mit den vom WDR im Rahmen der Beihilfeabrechnung überlassenen Mitarbeiterdaten umgeht. Es gab keine Beanstandungen seitens des Datenschutzes.

3. Datenschutz im Programm/ Onlinebereich sowie Medienforschung

3.1. Redaktionsdatenschutz

Nach den Enthüllungen von Edward Snowden und der Aufdeckung weiterer Abhörskandale haben wir uns intern im WDR und im Kreis der ARD-Kollegen seit 2013 auch verstärkt dem Thema Redaktionsdatenschutz gewidmet. Im Arbeitskreis der Datenschützer/innen von ARD und ZDF (AK DSB) haben wir uns u.a. mit Vertretern des Deutschen Presserates zu diesem Thema ausgetauscht. Wir waren uns einig, dass die Aktivitäten in- und ausländischer Geheimdienste

und die dabei eingesetzten Werkzeuge erwarten ließen, dass auch Journalistinnen und Journalisten Ziel von Ausspähungen sind bzw. sein können. Beim NDR war im September 2013 bereits der Fall eines freien Autors bekannt geworden, dessen Telekommunikationsdaten von der CIA abgefangen und dessen Arbeit und Reisetätigkeit von der CIA ausgeforscht worden sein sollen. Ins Visier der CIA ist der Kollege möglicherweise dadurch gelangt, dass er sich im Rahmen seiner journalistischen Tätigkeit auch mit Aktivitäten islamistischer Organisationen im Nahen Osten beschäftigte. Die konkreten Abhörmaßnahmen sollen während eines Aufenthaltes im Jemen stattgefunden haben. Ein Schreiben des NDR-Kollegen an den Botschafter der Vereinigten Staaten von Amerika in Deutschland, in dem darum gebeten wurde, bei der amerikanischen Regierung auf eine Aufklärung dieses Sachverhaltes hinzuwirken und über das wesentliche Ergebnis zu informieren, blieb ohne Beantwortung.

Dieser Vorgang ließ und lässt weiterhin befürchten, dass nicht nur der Informantenschutz nicht mehr gewährleistet werden kann, weil anhand von Verbindungsdaten festgestellt werden kann, wer mit dem betreffenden Journalisten Kontakt hatte und ihm möglicherweise für seine journalistische Tätigkeit wichtige Informationen geliefert hat. Im schlimmsten Fall würden Personen aufgrund des Kontaktes zu einem Journalisten überhaupt erst in den Fokus einer staatlichen Stelle. Damit wird die Aufmerksamkeit auf eine Person gelenkt, die nach deutschem Verfassungsrecht vor einer Preisgabe ihrer Identität besonders geschützt ist. Damit würde ein wesentliches Element einer funktionsfähigen freien Berichterstattung in Presse und Rundfunk nachhaltig gestört.

Gleichzeitig stellt auch die Berichterstattung über die Aktivitäten ausländischer Geheimdienste sowohl die Redaktionen als auch die IT-Sicherheit in den Rundfunkanstalten vor besondere Herausforderungen. Gemeinsam mit dem IT-Sicherheitsbeauftragten gibt es einen Austausch mit einzelnen Redaktionen - insbesondere den investigativ Tätigen – über die Bedrohungen durch Ausspähung von Daten und Maßnahmen zu deren Abwehr wie z.B. E-Mail- und Dateiverschlüsselung.

Um auch ein Zeichen nach außen zu setzen, sind wir im Arbeitskreis der Datenschutzbeauftragten von ARD und ZDF im Oktober 2013 mit folgender Pressemitteilung zum Redaktionsdatenschutz an die Öffentlichkeit gegangen:

„Datenschutzbeauftragte von ARD, ZDF und Deutschlandradio fordern Bund und Länder auf: Redaktionsdaten schützen!

Wer für den Schutz der Medien sorgt, schützt die Demokratie. Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten haben auf ihrer Jahrestagung am 25. Oktober 2013 in Berlin Bund und Länder aufgefordert, die Pressefreiheit zu schützen. Der Redaktionsdatenschutz als elementarer Bestandteil der Rundfunkfreiheit müsse verteidigt werden.

Die bekannt gewordenen Ausspähungen gefährden alle Bürger. Wenn aber Journalisten betroffen sind, gefährdet das zusätzlich die Aufgabe der öffentlich-rechtlichen Rundfunkanstalten bei der Informationsvermittlung und Meinungsbildung in unserer Gesellschaft. Die vertrauliche Kommunikation zwischen Journalisten und Informanten sowie die Recherchedaten müssen sowohl vor staatlichem Zugriff und als auch vor der Ausspähung durch ausländische Dienste bewahrt werden.

Die Datenschutzbeauftragten fordern Bund und Länder auf, gegen Verstöße wirksam vorzugehen. Gleichzeitig müsse eine flächendeckende Infrastruktur für eine gesicherte Kommunikation, zum Beispiel beim E-Mail-Verkehr, geschaffen werden.“

3.2. Einsatz des Online-Messverfahrens der Fa. Nielsen

Durch die zunehmende Online-Nutzung der TV-Angebote ist die klassische Reichweitenmessung (Einschaltquoten-Messung) ein immer ungenaueres Mittel der Medienforschung geworden. Die Arbeitsgemeinschaft Fernsehforschung (AGF), ARD, ZDF, ProSiebenSat.1 und die Mediengruppe RTL haben sich deshalb das Ziel gesetzt, auch die Nutzung von Bewegtbildinhalten (Mediatheken, Videos, etc.) über IP-basierte Dienste und Computer zu messen.

Ziel ist es, die Welt des klassischen Fernsehens einerseits und die Nutzung von Fernsehsendungen und sonstigen Bewegtbildinhalten über das Internet andererseits nach vergleichbaren Standards bewerten zu können und Überschneidungen oder Synergieeffekte messbar zu machen.

Da derartige Messverfahren u. a. an die IP-Adresse der Nutzer anknüpfen, werden bei der Nutzungsmessung grundsätzlich personenbezogene Daten verarbeitet. Ob es sich bei der IP-Adresse tatsächlich um ein personenbezogenes Datum handelt, war in der Vergangenheit umstritten, da nur der Zugangsprovider über die Information verfügt, welche konkrete IP-Adresse zu einem bestimmten Zeitpunkt welchem Teilnehmer zugeordnet ist. Der Europäische Gerichtshof hat jedoch in einer Entscheidung vom 24. November 2011 (EuGH,

Rechtssache C-70/10) diese Frage mit der Begründung bejaht, dass durch IP-Adressen eine genaue Identifizierung der Nutzer faktisch möglich sei. Damit werden bei Online-Messverfahren personenbezogene Daten verarbeitet mit der Konsequenz, dass hier auch die datenschutzrechtlichen Vorgaben zum Schutz von personenbezogenen Daten einzuhalten sind.

Konkret zu prüfen war der von der AGF und ihren Mitgliedern beabsichtigte Vertrag mit der deutschen Tochter des US-amerikanischen Marktforschungsunternehmens Nielsen. Da der WDR im Bereich Medienforschung die Federführung für diesen Vertrag innerhalb der ARD hatte, oblag mir als Datenschutzbeauftragter des WDR auch federführend die datenschutzrechtliche Prüfung, die ich gemeinsam mit meinem ZDF-Kollegen Christoph Bach vorgenommen habe.

Erfreulicherweise waren wir rechtzeitig eingebunden und konnten auf diese Weise unsere datenschutzrechtlichen Bedenken und Anforderungen bei den zuständigen Stellen sowie in die Verhandlungen einbringen und haben die entscheidenden Punkte auch durchsetzen können.

In den sich über mehrere Monate erstreckenden Verhandlungen konnten wir eine Festlegung auf die Einhaltung der europäischen und deutschen Datenschutzgesetze erzielen. Für das US-amerikanisch geprägte Unternehmen Nielsen war es eine Besonderheit, die Datenhaltung ausschließlich innerhalb der Europäischen Union vorzunehmen und die Daten auf einem von Nielsen genutzten Server in Paris zu hashen also unkenntlich zu machen. Entsprechend den rechtlichen Anforderungen haben wir gemeinsam mit dem ZDF vor Beginn der Datenverarbeitung eine vor-Ort-Kontrolle in Paris bei der Firma Nielsen und dem mit der Verarbeitung befassten Rechenzentrum vorgenommen und dokumentiert. Die Mustervereinbarung zur Auftragsdatenverarbeitung, die jede ARD-Anstalt, die von dem Messverfahren Gebrauch machen will, unterzeichnet, wurde mit Blick auf die datenschutzrechtlichen Anforderungen von uns entsprechend angepasst. Als wichtigsten Anforderungen sind das Verbot der Weitergabe personenbezogener Daten an Dritte und das oben bereits erwähnte Hashing der Daten am innereuropäischen Standort zu nennen. Weder bei Havarien noch bei back-ups dürfen Daten auf außereuropäische Server etwa in die USA gelangen.

Weiter haben wir innerbetrieblich sichergestellt, dass Nutzer des WDR-Onlineangebots in der Datenschutzerklärung des WDR darüber informiert werden, dass entsprechende Cookies für das Nielsen-Messverfahren eingesetzt werden, um statistische Analysen über die Nutzung dieser Webseite zu erstellen. Auch werden die user darauf hingewiesen, dass aufgrund des eingesetzten Verfahrens (Hashing) nur anonymisierte Nutzerinformationen erfasst werden, darüber hinaus aber auch eine Opt-Out-Funktion angeboten wird, mit der er oder sie sein/ihr Recht zum Widerspruch gegen die Verarbeitung der Daten nutzen und sich der Zählung entziehen kann.

4. Sonstiges

4.1. Einführung des elektronischen Dispositionssystems MIRAAN in der DPT

Dem Datenschutzreferat wurde im September 2014 mitgeteilt, dass die Abteilung DPT die bisher in Papierform durchgeführte Disposition von Produktionsmitteln und Planung von Einsatzmitteln durch ein elektronisches System (MIRAAN) ablösen möchte.
Nach eingehender datenschutzrechtlicher Prüfung kam ich zu dem Ergebnis, dass der Einführung von MIRAAN keine datenschutzrechtlichen Bedenken entgegenstehen.
Im Rahmen des für MIRAAN geltenden Berechtigungskonzepts ist der Zugriff auf die im System notwendigerweise enthaltenen personenbezogen Daten der Mitarbeiter/innen, die in der DPT für die verschiedenen Fernseh- und Hörfunkproduktionen disponiert werden, streng reglementiert. Es werden keine Daten an unbefugte Dritte weitergegeben oder durch nicht autorisierte Personen weiter bearbeitet. Die Daten befinden sich ausschließlich auf den WDR-eigenen Servern, es liegt ein Verfahrensverzeichnis und ein entsprechendes Löschkonzept vor.

4.2. SSL-Interception

Im Berichtszeitraum waren wir im Datenschutzreferat auch mit der Einführung von SSL- Interception befasst. Damit sollte eine Sicherheitslücke geschlossen werden, da bei verschlüsselten Verbindungen ohne SSL-Interception keine Virenprüfung am Übergang zum Internet stattfinden konnte und so Schadsoftware in das WDR-Netz hätte gelangen können. SSL-Interception stellt daher eine konsequente Weiterentwicklung der mehrstufigen Virenschutzstrategie des WDR dar.

Im Rahmen der Prüfung konnte ich mich davon überzeugen, dass der Einsatz von SSL-Interception zum Zwecke der Datensicherheit geeignet, erforderlich und verhältnismäßig ist. Zusammen mit Herrn Gust, dem IT-Sicherheitsbeauftragten des WDR, bin ich zu dem Ergebnis gelangt, dass ohne SSL-Interception eine wirksame Bekämpfung von Schadcodes zum Schutz der WDR- eigenen IT-Infrastruktur nicht möglich ist.

4.3. Fernwartungssoftware

Beim WDR war noch bis 2014 das Softwareverteilsystem Zenworks von der Fa. Novell im Einsatz. Durch den Wechsel des Betriebssystems von Windows XP auf Windows 7 sollte auch das Softwareverteilsystem geändert werden und zwar von Zenworks zu CCM (Center Configuration Manager) von Microsoft. Die Fernwartung ist bei diesem System ein fester Bestandteil.

Nach Auswertung und Prüfung der vorhanden Unterlagen zum geplanten Systemwechsel sowie der Auskünfte der zuständigen Abteilung IT-Services kam ich zu dem Ergebnis, dass der beabsichtigten Umstellung der Fernwartungssoftware keine Bedenken entgegenstehen.

Bei der datenschutzrechtlichen Prüfung konnte festgestellt werden, dass sich am bisherigen Verfahren der Fernwartung nichts änderte. Die Datenbestände bzw. Datenerhebung blieben identisch. Es wurden nicht mehr personenbezogene Daten als bisher und im Sinne der Aufgabe erforderlich durch die Abteilung IT-Services erhoben und verarbeitet. Alle Arbeitsschritte, die der Supporter aus der Ferne auf dem Rechner des Anwenders durchführt, sind für den Anwender sichtbar und bedürfen der vorherigen Einwilligung des/der Anwenders/in in die Aufschaltung von außen. Sämtliche Fernwartungssitzungen werden in einer zentralen Datenbank des WDR gespeichert. In der Datenbank werden Datum, Uhrzeit und Sitzungsaufbau gespeichert. Ebenso die Kennung des Administrators.

Auf Seiten des Anwenders wird lediglich der Rechnername gespeichert, zu dem die Verbindung aufgebaut wurde. Die Kennung des Anwenders wird nicht gespeichert. Die Einsichtnahme in diese Datenbank ist zweck- und aufgabenbezogen nur den Systembetreuern der Client-Entwicklung der Abteilung IT-S erlaubt bzw. möglich. Andere Supporter oder andere IT-Administratoren haben keinen Zugang zu diesen Daten. Ebenso gibt es keine neuen Einstellungen in der Konfiguration der Software CCM. Die Funktionsweise ist mit dem bisherigen eingesetzten Produkt der Fa. Novell nahezu identisch.

Dem Wechsel zur neuen Software Microsoft CCM bzw. dem dazugehörigen Tool zur Fernwartung standen daher aus datenschutzrechtlicher Sicht keine Bedenken entgegen

D. Datenschutz beim Beitragseinzug

1. Meldedatenabgleich und Änderung des Rundfunkbeitragsstaatsvertrags

Mit dem Inkrafttreten des 15. Rundfunkänderungsstaatsvertrages am 1.Januar 2013 hat der Wechsel von der geräteabhängigen Rundfunkgebühr zum geräteunabhängigen Rundfunkbeitrag stattgefunden. Dieser Wechsel hat zu veränderten Anzeigepflichten geführt. Anzuzeigen sind jetzt das Innehaben einer Wohnung, einer Betriebsstätte oder eines beitragspflichtigen Kraftfahrzeugs. Wenn der Inhaber nicht feststellbar ist, werden unter weiteren Voraussetzungen die Eigentümer der Wohnung oder des Grundstücks zu Angaben verpflichtet. Die Erhebung der Daten beim Betroffenen ist vorrangig; erst nachrangig und unter engen Voraussetzungen ist die Erhebung bestimmter erforderlicher Daten bei Dritten und ohne Kenntnis des Betroffenen zugelassen. So sieht § 11 Abs. 4 Rundfunkbeitragsstaatsvertrag vor, dass die zuständige Landesrundfunkanstalt im Wege des Ersuchens für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach dem Staatsvertrag besteht, personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis des Betroffenen erheben, verarbeiten oder nutzen kann. Von den Meldebehörden können jedoch nur bestimmte personenbezogene Daten wie Name, Alter und Anschrift ermittelt werden.

Jede Meldebehörde übermittelte in den Jahren 2013 und 2014 einmalig bestimmte personenbezogene Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt. Diese glichen die Daten mit den bei ihnen vorhandenen Daten ab, um etwaige nicht bekannte Beitragspflichtige zu erfassen. Für die Verwendung dieser Daten gelten strenge Voraussetzungen. Sobald für die fragliche Wohnung ein Beitragspflichtiger festgestellt und das für diese Wohnung geltende Beitragskonto ausgeglichen ist, hat die Landesrundfunkanstalt die Daten aller weiteren dort wohnenden Personen zu löschen.

Wie oben unter B 3 dargelegt, wurde die Rechtmäßigkeit des einmaligen Meldedatenabgleichs mehrfach gerichtlich bestätigt. Nun wird im Rahmen der Evaluierung des Rundfunkbeitrags und der Beratungen zum 16. Rundfunkänderungsstaatsvertrages über eine Wiederholung des vollständigen Meldedatenabgleichs nachgedacht. Die Datenschützer von ARD, ZDF und Deutschlandradio (AK DSB) halten eine Wiederholung des vollständigen Meldeabgleichs in einem Abstand von fünf bis sechs Jahren für datenschutzkonform, da kein ebenso geeignetes und milderes 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 zentrale Beitragsservice von ARD, ZDF und Deutschlandradio 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 Rundfunkbeitragsstaatsvertrages angeregt. Beispielsweise sollte eine Rechtsgrundlage für die Erhebung und Nutzung von Telefonnummern und E-Mail-Adressen aus öffentlich zugänglichen Quellen im nichtprivaten 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 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.

2. Anfragen und Auskunftsersuchen

Die betriebliche Datenschutzbeauftragte des zentralen Beitragsservice von ARD, ZDF und Deutschlandradio beantwortet im Auftrag der Datenschutzbeauftragten der einzelnen Landesrundfunkanstalten die an den zentralen Beitragsservice gestellten Fragen zum Datenschutz im Rahmen des Beitragseinzugs sofern es sich nicht um Grundsatzfragen handelt. Eingaben aus dem WDR-Sendegebiet oder datenschutzrechtliche Grundsatzfragen, die über den Routineschriftwechsel hinausgehen, beantworte ich selbst.

Eine Reihe von Anfragen zum Datenschutz beim Beitragseinzug gehen direkt bei mir ein oder werden vom Landesdatenschutzbeauftragten zuständigkeitshalber an mich zur Bearbeitung weitergeleitet. Das Gros dieser Anfragen richtete sich früher gegen die Mailingmaßnahmen der GEZ zur Ermittlung von Rundfunkteilnehmern sowie den Beauftragtendienst. Derartige Anfragen gehen inzwischen nicht mehr ein, da es den Landesrundfunkanstalten nach §14 Abs. 10 Rundfunkbeitragsstaatsvertrag bis zum 31.Dezember 2014 untersagt war, Adressdaten privater Personen anzukaufen. Darüber hinaus werden Regionalberater im Zuständigkeitsbereich des WDR nur noch im nicht-privaten Bereich eingesetzt.

Dennoch ist die Anzahl der Anfragen und Auskunftsersuchen von Rundfunkteilnehmern im Berichtszeitraum deutlich gegenüber den Vorjahren angestiegen. Bei den Eingaben und Anfragen steht nun häufig die Herkunft der gespeicherten Daten und die grundsätzliche Berechtigung zur Datenerhebung im Mittelpunkt des Interesses. Die Zahl der Bitten um Sperrung, Löschung oder Berichtigung der gespeicherten Daten zeigt eine deutlich steigende Tendenz. Dies ist meines Erachtens zum einen auf die Beitragsumstellung und den Meldedatenabgleich zurückzuführen, andererseits aber sicher auch auf das insgesamt deutlich erhöhte Bewusstsein und die Sensibilität für Themen der Datensicherheit und des Datenschutzes.

E. Zusammenarbeit und Informationsaustausch

1. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF, Deutschlandradio, Deutsche Welle und Beitragsservice (AK DSB)

Zur Koordinierung der datenschutzrechtlichen Kontroll- und Beratungstätigkeit im Bereich des öffentlich-rechtlichen Rundfunks treffen sich die Datenschutzbeauftragten von ARD, ZDF, Deutsche Welle, Deutschlandradio und die betriebliche Datenschutzbeauftragte des zentralen Beitragsservice zweimal jährlich. Zusätzlich werden besonders aktuelle und dringende Themen in Telefonschaltkonferenzen beraten. Dieses Rundfunk-Datenschutz-Forum, das seit 1979 besteht, bietet Gelegenheit Erfahrungen auszutauschen und anstaltsübergreifende Projekte gemeinschaftlich und zielgerichtet datenschutzkonform abzuwickeln. Hier werden auch die Interessen und Meinungen im Sinne der Mitwirkung bei gesetzgeberischen Vorhaben im Medien- und Datenschutzbereich gebündelt. Um einzelnen Themen in besonderem Maße gerecht zu werden, wirken verschiedene Mitglieder des AK DSB zusätzlich in themenbezogenen Unterarbeitskreisen mit. Darüber hinaus ist auch der Datenschutzbeauftragte des Österreichischen Rundfunks (ORF) mit dem AK DSB verbunden und nimmt regelmäßig an den Sitzungen teil.

Im zweijährigen Turnus wechselt der Vorsitz im Arbeitskreis. Im Berichtszeitraum 2013-2014 hatte der Datenschutzbeauftragte des ZDF, Herr Christoph Bach, den Vorsitz. Das Amt der Stellvertretung übt Herr Horst Brendel aus, Datenschutzbeauftragter des NDR. Seit 2009 nimmt auch ein Vertreter der Arbeitsgruppe Rundfunkgebühren bzw. Rundfunkbeitrag an den Sitzungen teil. Besonders für die datenschutzrechtlichen Themen des Beitragseinzugs sollen damit bereits in der Beratungsphase praxisnahe Informationen durch den Gast, Herr Christian Kramer (MDR), zur Verfügung stehen.

Zu den wichtigsten Themen, die im Berichtszeitraum im Arbeitskreis der Datenschutzbeauftragten von ARD und ZDF beraten wurden, gehören die Revision der EU-Datenschutz-Richtlinie / EU-Datenschutzgrundverordnung sowie der Minderjährigenschutz, der Leitfaden „Social Media Guidelines“, Mobile Apps sowie die Evaluierung des 15. Rundfunkänderungsstaatsvertrages. Im Bereich des Rundfunkbeitragseinzugs standen insbesondere der einmalige Meldeabgleich, das SEPA-Verfahren sowie zahlreiche Detailfragen der Anpassung an das neue Beitragssystem im Vordergrund.

2. Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder

Aus der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, einem freiwilligen Zusammenschluss der staatlichen Datenschutzbeauftragten, sind viele Arbeitskreise zu speziellen Themen hervorgegangen, unter anderem auch der Arbeitskreis Medien (AK Medien). Der AK Medien beschäftigt sich mit Themen speziell aus den Bereichen Datenschutz und Medien. Bei Themen von beiderseitigem Interesse, wird ein Vertreter des AK DSB zu den Sitzungen des AK Medien eingeladen. Im Berichtszeitraum hat den AK DSB und den AK Medien gemeinsam vor allem das Thema HbbTV beschäftigt.

3. Arbeitskreis IT-Sicherheitsgremium

Der Kollege Prof. Herb hat im SWR neben seiner Tätigkeit als Datenschutzbeauftragter inzwischen auch die Funktion des IT-Sicherheitsbeauftragten übernommen. Da er in dieser Funktion ordentliches Mitglied im IT-Sicherheitsgremium ist, hat er die Vertretung des AK DSB in diesem Gremium übernommen und berichtet regelmäßig über die Sitzungen im Kreis der Rundfunkdatenschutzbeauftragten.

Anhang

1. Pressemitteilung der AK DSB vom 25. Oktober 2013

Datenschutzbeauftragte von ARD, ZDF und Deutschlandradio fordern Bund und Länder auf: Redaktionsdaten schützen!

Wer für den Schutz der Medien sorgt, schützt die Demokratie. Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten haben auf ihrer Jahrestagung am 25. Oktober 2013 in Berlin Bund und Länder aufgefordert, die Pressefreiheit zu schützen. Der Redaktionsdatenschutz als elementarer Bestandteil der Rundfunkfreiheit müsse verteidigt werden.

Die bekannt gewordenen Ausspähungen gefährden alle Bürger. Wenn aber Journalisten betroffen sind, gefährdet das zusätzlich die Aufgabe der öffentlich-rechtlichen Rundfunkanstalten bei der Informationsvermittlung und Meinungsbildung in unserer Gesellschaft. Die vertrauliche Kommunikation zwischen Journalisten und Informanten sowie die Recherchedaten müssen sowohl vor staatlichem Zugriff und als auch vor der Ausspähung durch ausländische Dienste bewahrt werden.

Die Datenschutzbeauftragten fordern Bund und Länder auf, gegen Verstöße wirksam vorzugehen. Gleichzeitig müsse eine flächendeckende Infrastruktur für eine gesicherte Kommunikation, zum Beispiel beim E-Mail-Verkehr, geschaffen werden.

Der Arbeitskreis der Datenschutzbeauftragten (AK DSB) ist der Zusammenschluss unabhängiger Rundfunkbeauftragter für den Datenschutz von ARD, ZDF und Deutschlandradio.

Glossar

1. App

„App“ ist die Kurzform für das englische Wort „Application“ und lässt sich mit Anwendung“ übersetzen. Eine App ist eine Software,die auf mobilen wie stationären Endgeräten wie Smartphones, Tablets und Fernsehern und deren Betriebssystemen läuft.

Web App

Eine Anwendung, bei der im Zuge der Nutzung alle oder nur bestimmte Teile der Applikation aus dem Web geladen werden. Daher kann diese Anwendung in der Regel auf allen internetfähigen Endgeräten ausgeführt werden.

Natives App

Eine Anwendung, die nur auf einem bestimmten Endgerätetyp und dessen Betriebssystem lauffähig ist, wie zum Beispiel auf dem iPhone.

2. Datenschutz

Der Datenschutz hat das Ziel, jeden einzelnen Menschen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 BDSG). Datenschutz ist die Menge aller Vorkehrungen zur Verhinderung unzulässiger Informationsverarbeitung und umfasst jede Phase vom Beschaffen der Information über die Erfassung und Zusammenstellung bis zur Weitergabe oder Nutzung sowie der Veränderung oder Löschung.

3. Datensicherung und Datensicherheit

Damit der Datenschutz als rechtliches Ziel erreicht werden kann, sind technische und organisatorische Maßnahmen erforderlich. Sie werden mit den Begriffen „Datensicherung“ und „Datensicherheit“ umschrieben. Während mit dem Begriff „Datensicherung“ die Maßnahmen gemeint sind, wird die „Datensicherheit“ als das Ziel bezeichnet, das durch Datensicherungsmaßnahmen erreicht werden soll.

5. Fanpages
Fanpages sind Facebook-Seiten, auf denen sich beispielsweise Unternehmen, Künstlerinnen und Künstler oder Politikerinnen und Politiker darstellen und die in ihrem Aufbau und ihrer Funktion im Wesentlichen Facebook-Seiten privater Nutzer gleichen.

6. Personenbezogene Daten
Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse, die sich auf eine bestimmte oder bestimmbare Person beziehen. Im zuletzt genannten Fall spricht man auch von personenbeziehbaren Daten. Nach der Rechtsprechung des Europäischen Gerichtshofes und zahlreicher deutscher Gerichte ist die IP-Adresse einer Nutzerin/eines Nutzers ein personenbezogenes Datum. Dieser herrschenden Auffassung schließt sich der AK DSB an. Die sogenannte statische IP-Adresse
ermöglicht ohnehin stets eine Bestimmung der Anschlussinhaberin/des Anschlussinhabers. Über die sog. dynamische IP-Adresse ist eine Bestimmung des Anschlussinhabers mit verhältnismäßigem
Aufwand der datenverarbeitenden Stelle tatsächlich durchführbar, zumindest theoretisch stets möglich. Sensible personenbezogene Daten Sensible personenbezogene Daten sind zum Beispiel Angaben
über die ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben (§ 3 Abs. 9 BDSG).

7. Recht auf informationelle Selbstbestimmung
Grundsätzlich soll im Rahmen des aus Art. 2 Abs. 1, 1 Abs. 1 Grundgesetz (GG) abgeleiteten Rechts auf informationelle Selbstbestimmung jeder Einzelne selbst bestimmen können, welche Daten er von sich gegenüber wem preisgibt.

8. Social Media
Social Media beziehungsweise soziale Medien bezeichnen eine Vielfalt digitaler Medien und Technologien (Social Software), die es den Nutzerinnen und Nutzern ermöglicht, sich untereinander
auszutauschen und mediale Inhalte einzeln oder in Gemeinschaft zu gestalten.

9. Soziale Netzwerke
Soziale Netzwerke sind Netzgemeinschaften, die technisch durch Web-2.0-Anwendungen oder Portale unterstützt werden. Bestands- und Nutzungsdaten bei sozialen Netzwerken Bestandsdaten sind Daten, die für die Begründung der Mitgliedschaft in den sozialen Netzwerken erforderlich sind (vergleiche
§ 14 Abs. 1 TMG). Nutzungsdaten sind Daten, die die Aktivitäten im sozialen Netzwerk ermöglichen (Merkmale zur Identifikation der Nutzerinnen
und Nutzer, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angabe über die vom Nutzer in Anspruch genommenen Angebote, § 15 Abs. 1 TMG). Inhaltsdaten bei sozialen Netzwerken Inhaltsdaten sind alle personenbezogenen Daten der Nutzer, die sie selbst auf der Plattform des sozialen Netzwerks veröffentlichen und die nicht Bestands- oder Nutzungsdaten sind.

10. User-generated content
Inhalte, die nicht vom Anbieter eines Webangebots, sondern von dessen Nutzerinnen und Nutzern erstellt werden.

11. Widget
Unter Widgets werden Komponenten eines Fenstersystems verstanden.
Es handelt sich um kleine Elemente auf dem Desktop. Sie können zum Beispiel den Posteingang von E-Mail-Konten, die Uhrzeit, aktuelle Verkehrs- und Wettermeldungen oder aktualisierbare Nachrichtenschlagzeilen anzeigen. Grundlage eines
Widgets ist eine sogenannte Widget-Engine, eine Software, die die Voraussetzung für die Nutzung von Widgets bildet. Widget-Engines werden zum Beispiel von Apple, Google und Microsoft angeboten.

12. Zweckbindung
Grundsätzlich dürfen personenbezogene Daten nur für die Zwecke verarbeitet werden, für die sie erhoben wurden.

IMPRESSUM

Herausgeber
Westdeutscher Rundfunk Köln
Anstalt des öffentlichen Rechts
Datenschutzreferat
Appellhofplatz 1
50667 Köln

Redaktion
Beate Ritter
Datenschutzbeauftragte

Stand Februar 2016

WESTDEUTSCHER
RUNDFUNK

Appellhofplatz 1
50667 Köln

wdr.de