WDR

22.

TÄTIGKEITS BERICHT

der Datenschutzbeauftragten des WDR

Zeitraum 1. Januar 2011 bis 31. Dezember 2012

Inhaltsverzeichnis

Vorbemerkung

Am 1. Juni 2012 wurde ich durch den Rundfunkrat des Westdeutschen Rundfunks auf Vorschlag von Intendantin Monika Piel in Abstimmung mit dem Personalrat für die Dauer von fünf Jahren bis zum 31. Mai 2017 zur Datenschutzbeauftragten des WDR bestellt. 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 22. Tätigkeitsbericht dokumentiert den Zeitraum vom 1. Januar 2011 bis zum 31. Dezember 2012, der in wesentlichen Teilen noch in die Amtszeit meines Vorgängers, Herrn Thomas Drescher, fällt. Mit Herrn Drescher habe ich mich daher vor Erstellung des Berichts ausgetauscht. Im Tätigkeitsbericht werden allgemeine Entwicklungen des Datenschutzes sowie datenschutzrechtlich relevante Veränderungen und Problemstellungen im Westdeutschen Rundfunk während des Berichtszeitraums dargestellt.

Im Berichtszeitraum haben zunächst Herr Drescher und nachfolgend ich selbst uns intensiv mit datenschutzrechtlich relevanten Gesetzgebungsvorhaben auf europäischer sowie auf Bundes- und Landesebene beschäftigt. Hier ist vor allem der neue Rundfunkbeitragsstaatsvertrag im Rahmen des 15. Rundfunkänderungsstaatsvertrags zu nennen, der ab 2013 den Rundfunkgebührenstaatsvertrag abgelöst hat. Die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio haben das Gesetzgebungsverfahren intensiv begleitet. Gleiches gilt für die Vorbereitungsmaßnahmen der Rundfunkanstalten und des zentralen Beitragsservice mit Sitz in Bocklemünd 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 „Sitzanstaltsprinzips“ haben Herr Drescher und ich im Rahmen der sogenannten Controllboardsitzungen beim zentralen Beitragservice die Umstellung datenschutzrechtlich kritisch und intensiv begleitet.

Ein weiterer Tätigkeitsschwerpunkt war und ist die Novellierung der EU-Datenschutzrichtlinie und die Positionierung der öffentlich-rechtlichen Rundfunkanstalten im Novellierungsverfahren.

Was die Aktivitäten auf Landesebene angeht, war Herr Drescher in seiner Amtszeit auch mit der von der FDP-Fraktion eingebrachten Debatte über Kompetenzzuweisungen für den Datenschutz befasst.

Im Berichtszeitraum gab es erfreulicherweise keinen Anlass für förmliche Beanstandungen, die im Verfahren nach § 53 Abs. 3 WDR-Gesetz der Intendatin/dem Intendanten – bei gleichzeitiger Unterrichtung des Rundfunkrats – hätten mitgeteilt werden müssen.

Insgesamt ist festzustellen, dass die Themen Datenschutz und Datensicherheit im Bewusstsein der Mitarbeiterinnen und Mitarbeiter des WDR eine immer bedeutendere Rolle einnehmen. Ich werde in aller Regel schon präventiv in die jeweiligen Prozesse und Vorhaben eingebunden und um datenschutzrechtliche Einschätzung gebeten.

Bei meiner Tätigkeit als Datenschutzbeauftragte werde ich von meinem Stellvertreter und Mitarbeiter Herrn Günter Grießbach und von Frau Petra Baumann im Sekretariat unterstützt, denen ich an dieser Stelle für ihr kontinuierliches Engagement und die gute Zusammenarbeit ganz besonders danken möchte.

Ebenfalls danken möchte ich dem IT-Sicherheitsbeauftragten des WDR, Herrn Norbert Gust, dem Kollegen Roland Boysen im Justiziariat und der Datenschutzbeauftragten des zentralen Beitragsservice, Frau Kerstin Arens, für die stets kompetente, engagierte, und kollegiale Zusammenarbeit.

Köln, im Oktober 2013
Beate Ritter

A. Aufgaben der Datenschutzbeauftragten

Nach § 53 Abs. 1 WDR-Gesetz tritt der/die Beauftragte für den Datenschutz beim WDR an die Stelle des oder der Landesbeauftragten für den Datenschutz und die 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 Beitragsservice. Bei festgestellten Mängeln und Defiziten bestand in den betroffenen Abteilungen Bereitschaft zur Abhilfe. Meine Verbesserungsvorschläge wurden aufgenommen.

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

Dementsprechend bin ich verstärkt auch bei der Einführung WDR- oder ARD-weiter Verträge – insbesondere wenn die Federführung beim WDR liegt – bereits im Rahmen der Ausschreibung beteiligt worden und konnte die datenschutzrechtlichen Anforderungen, zum Beispiel an Streamingverträge, mitgestalten.

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

Die Informationen, die ich als Bürgerservice und als Hilfestellung auch über das Internetangebot des WDR eingestellt habe, sind dort weiterhin abrufbar. Auch das Intranetangebot der Datenschutzbeauftragten des WDR steht weiterhin für die Mitarbeiterinnen und Mitarbeiter bereit und wird regelmäßig aktualisiert und 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 Rundfunkteilnehmerinnen und -teilnehmer und auch Mitarbeiterinnen und Mitarbeiter Gebrauch, die sich wie andere Bürger schriftlich, telefonisch oder per E-Mail an mich wenden. Es geht dabei – wie in den vergangenen Jahren – nicht immer nur um datenschutzrechtliche Beschwerden. Vielfach werde ich auch um Auskünfte im Zusammenhang mit dem 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

Die derzeit noch geltende „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (EU-Datenschutzrichtlinie) stammt aus dem Jahr 1995. Sie zielt darauf ab, die Hindernisse für den freien Datenverkehr aus dem Weg zu räumen, ohne den Schutz personenbezogener Daten zu beeinträchtigen. Aufgrund dieser Richtlinie sollen die personenbezogenen Daten der EU-Bürgerinnen und Bürger in der gesamten Europäischen Union einen gleichwertigen Schutz genießen. Allerdings ist die Richtlinie insbesondere aufgrund der aktuellen technischen Entwicklungen und der damit verbundenen neuen Gefahren für den Datenschutz überarbeitungsbedürftig.

Zur Vorbereitung der Novellierung der EU-Richtlinie hat die EU-Kommission am 4. November 2010 die Mitteilung „Gesamtkonzept für den Datenschutz in der Europäischen Union“ veröffentlicht und interessierten Dritten die Möglichkeit zur Stellungnahme gegeben. In ihrer Mitteilung hat die EU-Kommission ihre Überlegungen für eine Reform des Datenschutzrechts ausführlich dargestellt und fünf Kernziele definiert, die durch eine Neuregelung des Datenschutzes auf europäischer Ebene erfüllt werden sollen:

\ Stärkung der Rechte des Einzelnen
\ Stärkung des EU-Binnenmarktes
\ Überarbeitung der Datenschutzbestimmungen im Bereich der Zusammenarbeit der Polizei- und Strafjustizbehörden
\ Gewährleistung eines hohen Schutzniveaus bei außerhalb der EU übermittelten Daten
\ Wirksamere Durchsetzung der Vorschriften

Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) hat sich intensiv mit diesem Konzept beschäftigt und ist dabei zu dem Ergebnis gelangt, dass insbesondere vor dem Hintergrund der technischen Fortentwicklung und globalen Vernetzung ein Harmonisierungsbedarf besteht, allerdings auch weiterhin der Einklang von Datenschutz und Meinungs-, Presse- und Rundfunkfreiheit gewährleistet sein muss.

Zu einem tragfähigen Gesamtkonzept für den Datenschutz in der EU gehörten auch die Beibehaltung und Absicherung des Medienprivilegs als Aufgabe der Mitgliedstaaten. Die ausführliche Stellungnahme des AK DSB zu dieser Mitteilung wurde über das Verbindungsbüro der ARD in Brüssel in den weiteren Normgebungsprozess eingespeist (vergleiche Anhang 1).

Ende 2011 sind die konkreten Regelungsvorschläge der EU-Kommission inoffiziell bekannt geworden. Daraufhin hat die Kommission ihre Vorschläge für ein revidiertes europäisches Datenschutzrecht am 25. Januar 2012 offiziell im Internet veröffentlicht.

ARD und ZDF begleiten das Neuordnungsverfahren intensiv über ihre Verbindungsbüros in Brüssel. Als Datenschutzbeauftragte des WDR bin ich hier ebenso einbezogen wie der NDR-Kollege, der sich innerhalb des Arbeitskreises der Datenschutzbeauftragten federführend um den europäischen Rechtssetzungsrahmen kümmert.

Aktuell hat der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments im Oktober 2013 über den Entwurf der Datenschutzgrundverordnung abgestimmt. Dabei hat sich der von ARD und ZDF unterstützte Ansatz durchgesetzt, der darauf abzielt, dass es in der Zuständigkeit der Mitgliedstaaten verbleibt, die Grundrechte auf Meinungs- und Informationsfreiheit sowie auf Datenschutz in Einklang zu bringen.

Die Positionierung im Parlament bietet damit auch eine gute Grundlage für die nun anstehenden Verhandlungen mit dem Rat. Ziel ist nach wie vor, eine vollständige Einigung noch in dieser Legislaturperiode zu erzielen. Das Europäische Parlament möchte im April 2014 in seiner letzten Plenarsitzung über das Dossier abstimmen.

Als Datenschutzbeauftragte der Landesrundfunkanstalten werden wir in diesem Reformprozess weiterhin das Ziel unterstützen, den Datenschutz zu stärken und dem Einzelnen eine bessere Kontrolle über seine Daten zu gewährleisten. Gleichzeitig werden wir aber auch im Sinne der öffentlich-rechtlichen Rundfunkanstalten darauf zu achten haben, dass durch die konkrete Formulierung der Regelungen auf europäischer Ebene nicht die Meinungsfreiheit sowie die Rundfunk- und Pressefreiheit wie auch die Stellung der Rundfunkdatenschutzbeauftragten infrage gestellt werden und es weiterhin bei einer staatsfernen Ausgestaltung bleibt.

Über den Fortgang des Reformprozesses auf europäischer und nationaler Ebene werde ich im kommenden Tätigkeitsbericht für die Jahre 2013 und 2014 berichten.

2. Bundesrecht

2.1 BESCHÄFTIGTENDATENSCHUTZ

Schon zur Amtszeit des Bundesministers Norbert Blüm (1982 – 1998) sollte ein Arbeitnehmerdatenschutzgesetz erlassen werden. Seit Jahren wird über die Notwendigkeit gesetzlicher Regelungen diskutiert. Mit den BDSG-Novellen des Jahres 2009 wurde ein erster Versuch unternommen, der allerdings nur dazu führte, dass jetzt eine generalklauselhafte Regelung in § 32 statt in § 28 BDSG besteht.

In der letzten Legislaturperiode ist man in Sachen Beschäftigtendatenschutz nicht zu einem Abschluss gekommen. Der Berichter-

stattung zu den aktuell laufenden Koalitionsverhandlungen ist aber zu entnehmen, dass man sich darauf geeinigt habe, den Arbeitnehmerdatenschutz zu verbessern. Man darf also auf die Fortsetzung des Themas in der neuen Legislaturperiode gespannt sein.

Für den WDR gilt indessen weiterhin § 29 Landesdatenschutzgesetz NRW zur Datenverarbeitung bei Dienst- und Arbeitsverhältnissen, welcher in Teilen auf beamtenrechtliche Regelungen verweist.

2.2 STOPP DES ELENA-VERFAHRENS

Mein Amtsvorgänger Thomas Drescher hatte in seinem letzten Tätigkeitsbericht über das ELENA-Verfahren berichtet. Danach waren sämtliche Arbeitgeberinnen und Arbeitgeber gesetzlich verpflichtet, monatlich eine entsprechende ELENA-Meldung an die bundesweit zentrale Speicherstelle (ZSS) zu versenden, damit die bisher von der Arbeitgeberin/Auftraggeber auf Papier erstellten Gehaltsbescheinigungen für Verfahren bei Sozialbehörden elektronisch zur Verfügung stehen.

Datenschützerinnen und Datenschützer hatten bereits während des gesamten Entstehungsprozesses erhebliche Bedenken angemeldet. Vor allem war bedenklich, dass Einkommensdaten von allen Beschäftigten, Beamtinnen und Beamten, Richterinnen und Richter und Soldatinnen und Soldaten zentral gespeichert werden, ohne dass feststand, ob die Daten im Einzelfall jemals gebraucht werden. Aus diesem Grund wurde ELENA von den Datenschutzbeauftragten des Bundes und der Länder sowie anderen Einrichtungen, insbesondere Gewerkschaften, als verfassungswidrige Datenspeicherung auf Vorrat kritisiert.

Auf einer Personalversammlung des WDR Personalrats kritisierten die anwesenden Beschäftigten ebenfalls

„das Datensammelgesetz ELENA in seiner jetzigen Form und forderten daher eine grundlegende Überarbeitung des Gesetzes. Das Gesetz sei nicht vereinbar mit dem verfassungsrechtlich geschützten Recht auf informationelle Selbstbestimmung und der ergangenen Rechtsprechung des Bundesverfassungsgerichtes.

Insbesondere die Menge der vorgesehenen Daten stehe nicht im Einklang mit dem Verhältnismäßigkeitsgrundsatz, die Gefahr des Missbrauchs werde dadurch noch verstärkt.“

Trotz der datenschutzrechtlichen Bedenken war das ELENA-Gesetz am 1. Januar 2010 in Kraft getreten. Am 18. Juli 2011 kündigte das Bundeswirtschaftsministerium jedoch die schnellstmögliche Einstellung von ELENA an. Begründet wurde der Schritt mit der fehlenden Verbreitung der elektronischen Signaturen. Zudem wurden die schnellstmögliche Löschung der erhobenen Daten sowie die Entlastung der Unternehmen mit dem Meldeverfahren verfolgt. Bereits im September 2011 verabschiedete das Bundeskabinett einen Entwurf zur Einstellung des vielfach kritisierten IT-Großprojekts und zur Löschung bereits erhobener Daten. Das entsprechende Gesetz wurde am 2. Dezember 2011 verkündet und trat am Folgetag in Kraft. Bereits wenige Tage später wurden sämtliche kryptografische Schlüssel zur Dekodierung der gespeicherten ELENA-Daten durch den Bundesbeauftragten für den Datenschutz Schaar vernichtet, der den Datenbankhauptschlüssel verwaltet hatte. Mittlerweile wurden die rund 700 Millionen gemeldeten Datensätze auch physikalisch gelöscht. Auch der WDR hat das Verfahren entsprechend datenschutzkonform eingestellt.

2.3 BUNDESMELDEGESETZ

Seit der Föderalismusreform hat der Bund die ausschließliche Gesetzgebungskompetenz für das Meldewesen (Art. 73 Abs.1. Nr. 3 GG). Am 31. August 2011 hat das Bundeskabinett beschlossen, diese Kompetenz wahrzunehmen und das Melderecht zu vereinheitlichen. Seit dem 16. November 2011 lag der Gesetzesentwurf vor. Am 28. Juni 2012 beschloss der Bundestag das Meldegesetz mit nur rund zwei Dutzend Abgeordneten in ca. 57 Sekunden. In seiner finalen Gesetzesfassung wurde den Meldebehörden gestattet, die persönlichen Daten der Bürgerinnen und Bürger an Firmen zu verkaufen, sofern kein ausdrücklicher Widerspruch der Bürgerin/des Bürgers vorlag.

Der Bundesrat schmetterte das heftig umstrittete Meldegesetz danach in seiner ersten Sitzung nach der parlamentarischen Sommerpause aus datenschutzrechtlichen Gründen ab. Nach dem Länderwillen sollte eine Weitergabe persönlicher Daten der Bürgerinnen und Bürger durch die Meldebehörden an Firmen, die daran ein werbliches Interesse haben oder damit handeln, nur mit Einwilligung der betroffenen Bürgerinnen und Bürger möglich sein. Im Vermittlungsausschuss einigten Bund und Länder sich im Februar 2013 darauf, dass eine ausdrückliche Zustimmung der Bürger nötig ist, wenn die Einwohnermeldeämter ihre Daten weitergeben wollen. Das entsprechend geänderte Bundesmeldegesetz wurde daraufhin im Mai 2013 verabschiedet worden und tritt am 1. Mai 2015 in Kraft.

Die Regelungen im Meldewesen sind für den WDR und die anderen Landesrundfunkanstalten insbesondere im Rahmen des Beitragseinzugs von Bedeutung.

3. Landesrecht

Im Zusammenhang mit dem Ratifizierungsverfahren des 15. Rundfunkänderungsstaatsvertrages, der insbesondere die Neuordnung der Rundfunkfinanzierung beinhaltet, brachte die Fraktion der FDP im nordrhein-westfälischen Landtag am 8. November 2011 den Entwurf eines „Gesetzes zur Entflechtung datenschutzrechtlicher Kompetenzen beim WDR“ (Drucksache 15/3261) ein. Ziel des Gesetzentwurfes sollte es sein, die Kontrolle über die Verarbeitung personenbezogener Daten aus dem Bereich des WDR durch die seinerzeitige GEZ im Zusammenhang mit der Einziehung von Rundfunkgebühren bzw. der jetzigen Rundfunkbeiträge dem staatlichen Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu übertragen. Somit sollte die Kompetenz des unabhängigen Rundfunkdatenschutzbeauftragten auf den journalistisch-redaktionellen Teil der Tätigkeit des WDR beschränkt werden.

Eine Verlagerung der Kontrolle der Verarbeitung personenbezogener Daten im administrativen Bereich des WDR stößt aber auf grundsätzliche verfassungsrechtliche Bedenken. So hat das Bundesverfassungsgericht in seiner Entscheidung zur Rundfunkfinanzierung über diesen Problemkreis hinaus allgemein festgelegt, dass die grundrechtlich bedingte Autonomie des öffentlich-rechtlichen Rundfunks nicht nur in inhaltlicher Hinsicht Staatsferne im Sinne einer Nichteinmischung staatlicher Stellen in die Programmgestaltung gebietet. Vielmehr muss auch sichergestellt werden, dass die Organisation des öffentlich-rechtlichen Rundfunks durch entsprechende Verfahren staatsfern erfolgt. Dieses Verfassungsgebot der Staatsferne führt konsequenterweise dazu, dass für den gesamten Tätigkeitsbereich des WDR eine dem Gebot der Staatsferne Rechnung tragende Kontrolle bei der Verarbeitung personenbezogener Daten durch einen eigenen, unabhängigen Datenschutzbeauftragten erforderlich ist.

In diesem Sinne hat auch die Intendantin des WDR seinerzeit gegenüber dem Präsidenten des Landtages NRW Stellung genommen.

Der Gesetzesentwurf wurde in der 48. Plenarsitzung des Landtages NRW kurz behandelt und an den Haupt- und Medienausschuss überwiesen. Durch die vorzeitige Beendigung der 15. Legislaturperiode wurde das Vorhaben nicht weiter behandelt und unter der jetzigen Landesregierung aus den vorgenannten verfassungsrechtlichen Gründen zurecht nicht wieder aufgegriffen.

C. Datenschutz im WDR

1. Allgemeines

1.1 AUSLAGERUNG DES RECHENZENTRUMS ZUR IVZ

Die Infrastruktur des Rechenzentrums (RZ) WDR, die Verwaltung und der Betrieb der zugehörigen Systeme wurden Ende 2011 im Rahmen des Projektes „Managed Service IVZ@WDR“ an das Informations-Verarbeitungs-Zentrum (IVZ) in Berlin übergeben. Das IVZ hat in Köln eine Niederlassung aufgebaut, sodass die räumliche Nähe zum RZ WDR weiter gegeben ist.

Das rechtlich unselbstständige Informations-Verarbeitungs-Zentrum (IVZ) wurde im Jahr 1993 als eine Gemeinschaftseinrichtung öffentlich-rechtlicher Rundfunkanstalten gegründet. Neben dem Westdeutschen Rundfunk (WDR) zählen der Norddeutsche Rundfunk (NDR), der Mitteldeutsche Rundfunk (MDR), der Saarländische Rundfunk (SR), der Rundfunk Berlin-Brandenburg (rbb), das Deutschlandradio und Radio Bremen (RB) zu den Kooperationspartnern.

Bei der IVZ werden für die beteiligten Anstalten, zentrale Aufgaben der elektronischen Datenverarbeitung wahrgenommen und durchgeführt. Für die Kontrolle des Datenschutzes und der Datensicherheit sind die Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Als zuständige Sitzanstalt ist hierbei die Datenschutzbeauftragte des rbb federführend. Beim IVZ ist auch ein betrieblicher Datenschutzbeauftragter bestellt.

Seit dem Zeitpunkt, zu dem die SAP-Systeme in die alleinige Verantwortung des IVZ übergegangen sind, steht dem WDR ein „Rund um die Uhr“-Support durch das IVZ zur Verfügung.

Das Projekt „Managed Service IVZ@WDR“ wurde in den gesamten Projektphasen unter datenschutzrechtlich relevanten Aspekten durchgeführt und vom Datenschutzreferat kritisch begleitet, das heißt, sämtliche Fragen, die den Datenschutz betreffen, wurden mit den zuständigen Verantwortlichen geklärt und umgesetzt. Die Datenschutzbeauftragten der beteiligten ARD-Anstalten informieren sich bei den regelmäßig stattfindenden Datenschutztreffen beim IVZ über den aktuellen Stand bezüglich IT-Sicherheit, etwaigen Störfällen, deren Ursachen und Auswirkungen sowie zu anderen datenschutzrechtlich relevanten Fragen.

1.2 IVZ-STÖRFÄLLE

Bei der Datenschutztagung des IVZ am 24. November 2012 in Berlin wurde der Datenschutz erstmals über Störfälle informiert, die den Zeitraum 2011 – 2012 betrafen. Um die Vorfälle aufzuklären, wurden diese eingehend von Herrn Grießbach sowie von Herrn Gust, dem IT-Sicherheitsbeauftragten, geprüft und begutachtet, um eine lückenlose Aufklärung der Störfälle zu erhalten.

In der Folge dieser Überprüfung haben wir bei den Verantwortlichen des IVZ auf eine Überprüfung des Benachrichtigungsworkflows bei Störfällen gedrungen, da die Störfälle nicht zeitnah bearbeitet beziehungsweise gemeldet worden waren. Dies ist inzwischen geschehen. Um in Zukunft schneller auf Störfälle reagieren zu können, werden die Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte des WDR künftig bei Störfällen unverzüglich vom IVZ in Kenntnis gesetzt, sofern die Störfälle die IT-Sicherheit und den Datenschutz betreffen beziehungsweise gefährden.

Darüber hinaus wurde vereinbart, dass die IT-Services, die IT-Sicherheit und das Datenschutzreferat künftig jährlich zu einem Informationsaustausch im IVZ zusammenkommen.

Aus Sicht des Datenschutzes bleibt festzuhalten, dass alle Störfälle ausgeräumt und geklärt werden konnten und es zukünftig durch die schnellere Benachrichtigung durch die zuständigen Stellen keine Verzögerungen in der Bearbeitung mehr geben dürfte.

1.3 EINFÜHRUNG DYNAMISCHER WEBFILTER ZUM SCHUTZ VOR SCHÄDLICHEN WEBSEITEN

Durch die zunehmende Verbreitung der elektronischen Medien (Internet, soziale Netzwerke, E-Mail, et cetera.) wird mittlerweile immer mehr Schadsoftware durch unsicher konfigurierte Webseiten verbreitet. Eine bewährte Strategie, sich vor solchen Webangriffen zu schützen, ist die Nutzung sogenanter dynamischer Webfilter. Hierbei werden Webseiten, die Schadsoftware oder Hackerwerkzeuge verbreiten, mithilfe ständig aktualisierter Listen gesperrt. Die Listen werden – vergleichbar mit dem im WDR bereits eingesetzten Spamfilter – vom Hersteller tagesaktuell gepflegt und bieten somit einen zeitnahen Schutz auch vor wechselnden URLs. So kann das ungewollte Nachladen von Schadsoftware aus dem Internet verhindert werden.

Bei MDR und ZDF werden solche Filter bereits seit einiger Zeit mit Erfolg eingesetzt. Auch andere Rundfunkanstalten planen den Einsatz. Die AG IT-Sicherheit unterstützt diese Maßnahme ebenfalls und hält sie für eine notwendige Erweiterung des Schutzes des WDR vor Bedrohungen durch Schadsoftware aus dem Internet.

Die Abteilung IT-Services wurde daher gebeten, die vorhandene Proxy-Infrastruktur um entsprechende dynamische Webfilter zu erweitern und sicherzustellen, dass eine Filterung von Webinhalten nur zu dem vereinbarten Zweck stattfindet. Hierbei waren u.a. folgende Fragestellungen zu klären und datenschutzrechtskonform auszugestalten:

\ Streng zweckgebundene Eingrenzung der Module und Filterkriterien
\ Sicherheit der Verbindung zwischen WDR-IT und Webfilter
\ Die Webfiltertechnik darf keine Erkenntnisse über das Surfverhalten der WDR-User ermöglichen
\ Die Webfiltertechnik darf keine Leistungs- und Verhaltenskontrolle ermöglichen et cetera.

Die datenschutzrechtlich relevanten Punkte wurden mit den zuständigen Fachbereichen erörtert und entsprechend den Empfehlungen umgesetzt, sodass es vonseiten des Datenschutzes keine Beanstandungen zu Einführung des Webfilters gab.

2. Datenschutz im Personalbereich

2.1 DIENSTPLÄNE

Wie gehe ich mit den Daten von Kolleginnen und Kollegen auf Dienstplänen um? In vielfältiger Form finden sich im WDR Einsatzpläne einzelner Abteilungen. Mal als reine Urlaubsplanung, mal in Form einer detaillierten Einsatzübersicht dienen diese Pläne der Arbeitsorganisation und als Information für die Betroffenen. Die Pläne werden zum Teil in den Abteilungen ausgehängt.

Einblick in Tabellen mit personenbezogenen Daten durch nicht autorisierte Personen ist datenschutzrechtlich bedenklich und muss vermieden werden. Bei der Nutzung von Personaübersichten in den Abteilungen sind folgende datenschutzrechtliche Maßgaben einzuhalten:

\ Der Nutzerkreis muss ausschließlich auf die betroffenen Personen eingegrenzt werden.
\ Die Rechtevergabe für Schreiben, Lesen und Drucken der Dienstpläne muss nach der strengen Maßgabe arbeitsplatzbezogener Relevanz erfolgen.
\ Grenzenlose Datenspeicherung ist durch entsprechende Löschroutinen zu unterbinden.
\ Der Abwesenheitsgrund (zum Beispiel Fortbildung, Teilzeit, Kuraufenthalt, Krankenstand) einer Mitarbeiterin/eines Mitarbeiters darf auf den Einsatzplänen nur für die Personalreferentinnen und Personalreferenten und Vorgesetzten ersichtlich sein. Insbesondere die sensiblen Gesundheitsdaten unterliegen einem hohem Schutz. Für alle anderen Nutzerinnen und Nutzer der Pläne darf lediglich der Tatbestand der Abwesenheit erkennbar sein.

Im Berichtszeitraum habe ich unter anderem in einem Bereich die Einführung einer Software zur Abwesenheits- bzw. Urlaubsplanung beratend begleitet, mit dem Ergebnis, dass diese nach den oben genannten Kriterien datenschutzkonform ausgestaltet wird.

2.2 VIDEOÜBERWACHUNG

Den Skandalen im Bereich des Datenschutzes ist es zu verdanken, dass die Sensibilität für die eigenen Persönlichkeitsrechte gestiegen ist. Beim Stichwort Videoüberwachung wird so manch einer hellhörig. Sicherheitsaspekte stehen hier dem Eingriff in das

Persönlichkeitsrecht gegenüber. Als Ausfluss des Rechts auf informationelle Selbstbestimmung darf jeder über die Preisgabe und Verwendung seiner persönlichen Daten selbst bestimmen. Wenn also mit einer Kamera auch Bilder von Personen aufgezeichnet werden können, über die eine Person bestimmbar ist, muss der Einsatz dieser Kamera im überwiegenden Allgemeininteresse liegen, das den Eingriff in das Persönlichkeitsrecht der erfassten Personen rechtfertigt. Denn im Falle der Videoüberwachung können die auf dem Bild erfassten Personen nicht selbst über die Datenerhebung und -verarbeitung bestimmen.

Der Gesetzgeber hat in § 6b BDSG und entsprechend auf Landesebene in § 29b LDSG NRW den Einsatz nichtpolizeilicher Überwachungskameras in öffentlich zugänglichen Räumen geregelt. So ist insbesondere vorgeschrieben, den Umstand der Beobachtung erkennbar zu machen. Ist der Zweck der Videoüberwachung erfüllt, sind die Videoaufzeichnungen unverzüglich zu löschen.

Im WDR werden in einigen Bereichen Videokameras eingesetzt. Immer wieder erreichen mich Anfragen, wie datenschutzkonform mit solchen Kameras zu verfahren sei.

Der Gesetzgeber hat mit der Schaffung des § 29b LDSG NRW, die Videoüberwachung für öffentliche Stellen speziell geregelt. Diese Vorschrift regelt nicht nur die Erhebung personenbezogener Daten durch optisch-elektronische Einrichtungen (Videokamera oder Webcams), sondern umfasst auch die Speicherung und weitere Verwendung der erhobenen Daten. Ich möchte hier die wichtigsten Voraussetzungen für einen gesetzeskonformen Einsatz von Überwachungskameras zusammengefasst darstellen, an denen ich mich auch bei entsprechenden Anfragen aus dem Haus orientiere:

\ Der Zweck der Videoüberwachung muss begründet werden, ebenso die räumliche Ausdehnung der Aufzeichnung und der zeitliche Umfang der Überwachung.
\ Jeder Einsatz von Überwachungskameras bedarf der vorherigen Prüfung durch mich als Datenschutzbeauftragte und der schriftlichen Freigabe durch die verantwortliche Stelle.
\ Ein Hinweis auf die Videoüberwachung ist erforderlich.
\ Die Speicherdauer der Aufzeichnungen richtet sich nach der Notwendigkeit der Überwachung des betroffenen Bereiches und ist in angemessenen Zeitabständen zu überprüfen.

2.3 PRÜFUNG DER BADEN-BADENER PENSIONSKASSE

Die Baden-Badener Pensionskasse ist vom WDR wie auch von anderen Landesrundfunkanstalten mit der Abwicklung der Versorgungsleistungen seiner Arbeitnehmerinnen und Arbeitnehmer beauftragt. Sie wurde 1998 als Versicherungsverein auf Gegenseitigkeit gegründet. Mitglieder sind die Landesrundfunkanstalten sowie deren Tochter- und Beteiligungsgesellschaften. Die Datenschutzkontrolle wird vom Datenschutzbeauftragten der sitzgebenden Anstalt SWR, Herrn Prof. Dr. Armin Herb, vorgenommen, der in regelmäßigen Abständen Prüfungen durchführt. Die Empfehlungen des Kollegen Herb an die Baden-Badener Pensionskasse aus der letzten Prüfung im Dezember 2012 befinden sich in der Umsetzung.

Darüber hinaus bemühe ich mich derzeit gemeinsam mit den für die Vertragsgestaltung zuständigen Kolleginnen und Kollegen beim NDR, bislang noch fehlende datenschutzrechtliche Regelungen auch in den Vertrag zwischen ARD und der Baden-Badener Pensionskasse aufzunehmen.

3. Datenschutz im Programm-/ Onlinebereich

3.1 MINDERJÄHRIGENSCHUTZ

Der öffentlich-rechtlichen Rundfunk und besonders der WDR bietet Kindern programmlich wie auch medienpädagogisch hochkarätige Angebote in Hörfunk, Fernsehen wie auch in seinen Onlineangeboten. Mit Programmangeboten wie der „Sendung mit der Maus“, dem Kiraka, dem Ohrenbären, KiKa et cetera. hebt sich der öffentlich-rechtliche Rundfunk mit seinen Kindersendungen deutlich von kommerziellen Sendern und deren Angeboten ab, die wesentlich auf die werbliche Beeinflussung der Kinder abzielen. Ganz im Gegensatz hierzu sind die öffentlich-rechtlichen Angebote darauf ausgerichtet, den Kindern und Jugendlichen ein hochwertiges, intelligentes und attraktives Programm zu bieten. Vielmehr stärken sie auch die Medienkompetenz des jungen und jüngsten Publikums und geben Ihm Orientierung im Umgang mit den vielfältigen Informations- und Medienquellen, die Ihm zur Verfügung stehen.

In diesem Zusammenhang spielt auch der datenschutzkonforme Umgang mit den Daten von Kindern und Jugendlichen, die sich an den Programmangeboten der Landesrundfunkanstalten beteiligen, eine wichtige Rolle. Meine Gespräche mit den Programmmacherinnen und Programmmacher von Kindersendungen und Onlineangeboten haben gezeigt, dass bereits eine hohe Sensibilität für dieses Thema besteht und auch bei Zweifelsfragen der Kontakt zur Datenschutzbeauftragten gesucht wird.

Datenschutzrechtlich befinden wir uns im Minderjährigenschutz aber in einem Bereich, für den es keine feststehenden Regeln und keine Rechtsprechung gibt, ab wann die grundsätzlich erforderliche Elterneinwilligung entbehrlich ist, etwa weil von der Einsichtsfähigkeit des Kindes/Jugendlichen auszugehen ist oder weil das Mitmachen bei einem Programmangebot dem Umgang des Kindes mit elektronischen Medien und seiner (medialen) Bildung ausschließlich zum Vorteil gereicht. Hinzu kommt, dass es auch eine Vielzahl von Fallgestaltungen gibt, die sich sowohl an unterschiedliche Altersgruppen wenden als auch unterschiedlich sensible personenbezogene Daten der Kinder und Jugendlichen betreffen.

Auch mit Blick auf die Entwicklungen zum Minderjährigenschutz im Rahmen der Neuordnung des Datenschutzes auf europäischer Ebene haben wir uns im AK DSB (Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio) mit dem Thema näher befasst, zumal die derzeit im Entwurf der EU-Datenschutzverordnung vorgesehene Grenze bei 13 Jahren liegt. Dies entspricht „zufälligerweise“ auch dem Eintrittsalter für Facebook. Schlimmstenfalls könnte eine solche Regelung zur Folge haben,

dass Kinder und Jugendliche bis 13 Jahre an den programmlich und pädagogisch wertvollen Angeboten von ARD und ZDF nur mit vorheriger schriftlicher Elterneinwilligung partizipieren können, während dies für die Facebooknutzung entfiele.

Besonders betroffen sind dabei Angebote, die Kinder und Jugendliche nur dann sinnvoll nutzen können, wenn sie zeitlich unmittelbar, ohne Medienbruch und damit ohne schriftliche Einverständniserklärung der Eltern teilnehmen können, zum Beispiel die Call-in-Sendungen, Gästebüchern et cetera. Neben dem eigentlichen pädagogischen Angebot ist hiermit auch die Förderung der Medienkompetenz verbunden, da Kinder ohnehin den selbstverständlichen Umgang mit den Medien heute fast schon zwangsläufig einüben. Insofern wäre es äußerst wünschenswert, dass gerade die Angebote des öffentlich-rechtlichen Rundfunks an dieser Stelle nicht zurückstehen, sondern praxistaugliche Möglichkeit für die Kinder und Jugendlichen bieten, sich auf sicherem Terrain im Internet zu bewegen.

In einer Unterarbeitsgruppe des AK DSB arbeite ich zur Zeit gemeinsam mit anderen Rundfunkdatenschutzbeauftragten an einem Leitfaden zum Datenschutz bei Kindern und Jugendlichen, mit dem wir den Programmmacherinnen und Programmmacher eine Orientierung für die datenschutzrechtlichen Anforderungen unterschiedlicher Programm-Angebotskategorien für Kinder und Jugendliche geben wollen. Der Leitfaden orientiert sich an der altersgemäßen Einsichtsfähigkeit von Kindern und Jugendlichen, bezieht aber auch den Gesichtspunkt ein, wann ein Angebot für Kinder so geeignet und medienpädagogisch wertvoll ist, dass eine Teilnahme nicht nur als unschädlich sondern sogar als förderlich angesehen werden kann. Dementsprechend können die Kinder und Jugendlichen ohne Elterneinwilligung an bestimmten Angeboten teilnehmen Selbstverständlich wird es je nach Sensibilität der Daten immer auch Angebote geben, bei denen die schriftliche Elterneinwilligung erforderlich ist.

Der Leitfaden befindet sich noch in Arbeit, zumal wir hier die Expertise der Jugendschutzbeauftragten einbeziehen wollen, deren Kompetenzen und Kenntnisse gerade für die Frage der medienpädagogischen Qualität und der Einsichtsfähigkeit aus unserer Sicht eine wichtige Rolle spielen. Über den Fortgang werde ich im nächsten Tätigkeitsbericht informieren.

3.2 DATENSCHUTZ UND INTERNET

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik stetig gestiegen, zumal Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden.

Vor allem durch die globale Vernetzung im Internet haben die Gefahren für den Schutz personenbezogener Daten immens zugenommen. Möglichkeiten der Datenverlagerung (zum Beispiel Outsourcing, Offshoring, Cloud), weltweite Servernetze maßgeblicher IT-Dienstleister sowie Verlagerungen von IT-Aufgaben in Regionen, in denen deutsche und europäische Gesetze weder gelten noch durchsetzbar sind und ausländische Regierungsbehörden Zugang zu Daten haben, bereiten der Durchsetzung von Datenschutz in der Praxis erhebliche Probleme.

Der WDR muss sich deshalb zunehmend nicht nur mit den grundlegenden Fragen des technischen Datenschutzes (Datensicherheit), sondern auch mit der effektiven Durchsetzbarkeit von Datenschutz für den Bereich des öffentlich-rechtlichen Rundfunks auseinandersetzen, um personenbezogene Daten vor unerlaubten Zugriffen zu schützen. Ein zentrales Thema ist hierbei der Informanten- und Redaktionsdatenschutz, der aktuell – auch aufgrund des NSA-Skandals und der Ausspähaffäre – einen besonderen Arbeitsschwerpunkt im Arbeitskreis der Datenschutzbeauftragten darstellt. Mehr Informationen dazu folgen im Tätigkeitsbericht für die Jahre 2013/2014.

Ebenso wichtig ist aber auch die Einhaltung des Datenschutzes durch den WDR im Verhältnis zu seinem Publikum. Erfreulicherweise werde ich bei der Ausschreibung von Verträgen mit datenschutzrelevanten Leistungen (zum Beispiel Streamingverträgen) bereits im Vorfeld einbezogen. Datenschutzrechtliche Anforderungen spielen damit schon von vornherein sowohl bei der Auswahl der Vertragspartner als auch bei der Ausgestaltung der Verträge eine Rolle.

Insbesondere bei den Onlineangeboten des WDR, den Apps und der Medienforschung, die auch im Onlinebereich ein wichtiges Instrument zur Akzeptanzüberprüfung ist, ist der WDR den Userinnen und Usern nicht nur einen datenschutzkonformen Umgang mit deren Daten schuldig. Auch die Transparenz des Umgangs mit diesen Daten, ist unerlässlich. Für mich als Datenschutzbeauftragte ist dies ein Bereich, in dem ich mit den zuständigen Redaktionen und Bereichen daran arbeite, dass die datenschutzrechtlichen Anforderungen von Anfang an erfüllt werden und die notwendige Transparenz durch entsprechende Hinweise im Internet geschaffen wird.

Mit seiner Onlinedatenschutzerklärung, die wir im Berichtszeitraum neu erstellt haben, klärt der WDR die Nutzer seiner Onlineangebote darüber auf, in welchen Fällen, für welche Zwecke und in welchem Umfang gewisse personenbezogene Daten (zum Beispiel IP-Adressen bei der Medienforschung) erfasst werden, was mit diesen geschieht und wie die Userin/der User user z.B. das Setzen von Cookies durch ein opt-out verhindern kann. Der WDR erfasst personenbezogene Daten nur im Rahmen gesetzlicher Vorgaben, die unter anderem im LDSG NRW oder im Telekommunikationsgesetz (TKG) verankert sind.

3.3 AKTUALISIERUNG SOCIAL-MEDIA-LEITFADEN

Aufgrund der weiterhin zunehmenden Bedeutung der sozialen Netzwerke für die Wahrnehmung und Verbreitung der Programmangebote des WDR insbesondere beim jungen Publikum, hat der Arbeitskreis der Rundfunkdatenschutzbeauftragten von ARD, ZDF und Deutschlandradio Richtlinien für eine datenschutzkonforme Gestaltung sozialer Netzwerke erarbeitet. Dieser Leitfaden, der im WDR publiziert ist, ist als Orientierung gedacht und ersetzt nicht in allen Fällen die Beratung der Redaktionen durch die Datenschutzbeauftragte, von der auch weiterhin Gebrauch gemacht wird. In Anhang 2 ist die aktuelle Fassung des Social-Media-Leitfadens beigefügt.

D. Datenschutz beim Beitragseinzug

1. Rundfunkbeitragsstaatsvertrag und einmaliger Meldedatenabgleich

Im letzten Tätigkeitsbericht hat mein Amtsvorgänger, Thomas Drescher, unter Punkt 3.8 ausführlich über die datenschutzrechtlichen Aspekte im Zusammenhang mit der Neuordnung der Rundfunkfinanzierung durch den 15. Rundfunkänderungsstaatsvertrag berichtet. Wesentliche Neuerung des nunmehr seit dem 1. Januar 2013 geltenden Rundfunkbeitragsstaatvertrages ist die Einführung eines geräteunabhängigen Rundfunkbeitrages anstelle der bisherigen geräteabhängigen Rundfunkgebühr.

Die Neuregelungen sind zum Teil durchaus datenschutzfreundlicher, weil zum Beispiel die bisherigen Nachforschungen bei den Bürgerinnen und Bürgern zum Bereithalten von Rundfunkgeräten weitgehend entfallen konnten. Auch elementare datenschutzrechtliche Vorgaben wie die vorrangige Direkterhebung von Daten bei Betroffenen bleiben gewahrt.

Allerdings bedurfte es zur Sicherstellung des erforderlichen Schutzes bei der Erhebung und Verarbeitung personenbezogener Daten im Rahmen der Erarbeitung des Staatsvertragsentwurfes eines intensiven Austausches zwischen den Staats- und Senatskanzleien, den Rundfunkanstalten, den Landesdatenschutzbeauftragten und den Rundfunkdatenschutzbeauftragten. Zu diesem Zweck hat der AK DSB eine Stellungnahme zu den datenschutzrechtlich relevanten Bestimmungen des Entwurfs des 15. Rundfunkänderungsstaatsvertrages abgegeben (vergleiche Anhang 3). Den wichtigsten datenschutzrechtlichen Erfordernissen, die in dieser Stellungnahme dargelegt werden, wurde beim Rechtssetzungsverfahren Rechnung getragen.

In der Kritik stand uunter anderem der einmalige Meldedatenabgleich mit den Meldebehörden nach § 14 Abs. 9 Rundfunkbeitragsstaatsvertrag zum Zwecke der Bestands- und Ersterfassung von Beitragsschuldnern. Zwar hat der Gesetzgeber 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 Beitragsschuldnerinnen und -schuldner im Sinne einer größeren Beitragsgerechtigkeit ist es auch erforderlich, dass Beitragsschuldnerinnen und -schuldner nicht nur einer bestimmten Adresse, sondern auch einer konkreten Wohnung zugeordnet werden können (vergleiche auch §§ 2 Abs. 1, 3 Abs. 1 Rundfunkbeitragsstaatsvertrag).

Inzwischen hat der Bayerischer Verfassungsgerichtshof 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 Beitragsschuldnerin/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 Beitragsschuldnerin/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.

2. Anfragen und Auskunftsersuchen

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

Eine Reihe von Anfragen zum Datenschutz beim Rundfunkgebühreneinzug gehen direkt bei mir ein oder werden vom Landesdatenschutzbeauftragten und vom Bundesdatenschutzbeauftragten zuständigkeitshalber an mich zur Bearbeitung weitergeleitet. Das Gros dieser Anfragen richtete sich früher gegen die Mailingmaßnahmen der GEZ zur Ermittlung von Rundfunkteilnehmerinnen und -teilnehmern sowie den Beauftragtendienst. Für die bei mir eingehenden Auskunftsersuchen ist festzustellen, dass derartige Anfragen deutlich nachgelassen haben. Dies dürfte zum einen daran liegen, dass es den Landesrundfunkanstalten nach §14 Abs. 10 Rundfunkbeitragsstaatsvertrag bis zum 31. Dezember 2014 untersagt ist, Adressdaten privater Personen anzukaufen. Darüber hinaus werden Regionalberaterinnen und -berater im Zuständigkeitsbereich des WDR nur noch im nichtprivaten-Bereich eingesetzt.

Bei den Eingaben und Anfragen, die mich als Datenschutzbeauftragte erreichen, stehen 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 leicht steigende Tendenz, was vermutlich auf das deutlich erhöhten Bewusstsein und die Sensibilität für Themen der Datensicherheit und des Datenschutzes in der gesamten Bevölkerung zurückzuführen ist.

E. Zusammenarbeit und Informationsaustausch

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

Auch im Berichtszeitraum 2011/2012 haben sich die Rundfunkdatenschutzbeauftragten wieder regelmäßig im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF, Deutschlandradio, Deutsche Welle und Beitragsservice (AK DSB) getroffen. Diese Sitzungen stellen einen regelmäßigen Kontakt zwischen den einzelnen Mitgliedern sicher und ermöglichen einen Erfahrungsaustausch und eine Kooperation in gemeinsamen Vorhaben.

So trafen sich die Mitglieder des AK DSB am 5./6. Mai 2011 bei Radio Bremen und am 10./11. November 2011 bei der Deutschen Welle in Bonn. Zur Klärung von Fragen im Zusammenhang mit Änderungen durch die Einführung des neuen Rundfunkbeitrags wurde eine Sondersitzung am 12. September 2011 bei der GEZ in Köln einberufen. Im Jahr 2012 fanden zwei weitere reguläre Sitzungen des AK DSB am 26./27. April 2012 beim WDR in Köln und am 20./21. September beim MDR in Dresden statt.

Den Vorsitz des Arbeitskreises hatte für die Jahre 2011 und 2012 Herr Brendel vom Norddeutschen Rundfunk inne. Im Berichtszeitraum nahm auch ein Vertreter der AG Rundfunkgebühren regelmäßig an den Sitzungen des AK DSB teil. Auf diese Weise wird die Zusammenarbeit mit den für den Rundfunkgebühreneinzug zuständigen Bereichen gefördert und es steht ein Ansprechpartner aus der Praxis für Diskussionen zu Gebührensachverhalten zur Verfügung. Insbesondere im Hinblick auf die Änderung vom Gebühren- auf das Beitragsmodell hat sich die Zusammenarbeit intensiviert.

Seit 2009 nahm zudem die Vorsitzende des Arbeitskreises Medien der staatlichen Datenschutzbeauftragten, die Datenschutzbeauftragte des Landes Brandenburg, Frau Hartge, an einem gemeinsamen Teil der Sitzung teil. Hierdurch sollen die Zusammenarbeit und der Erfahrungsaustausch zu speziellen Themen aus den Bereichen Datenschutz und Medien gefördert und verbessert werden.

Neben dem Meinungs- und Informationsaustausch wird insbesondere für Fragen, die über die jeweilige Rundfunkanstalt hinaus Bedeutung aufweisen, eine einheitliche Handhabung und Problemlösung angestrebt. Im AK DSB wurden in den vergangenen zwei Jahren dabei regelmäßig insbesondere folgende Themen behandelt:

Gesetzgebung und Rechtsprechung:
\ Entwicklungen auf europäischer Ebene (Art. 29-Gruppe; siehe hierzu auch Punkt 2.1.1)
\ Arbeitsgruppe nach Art. 29 EG-Datenschutzrichtlinie
\ Vorratsdatenspeicherung
\ Eckpunktepapier des BMI zum Beschäftigtendatenschutz

GEZ bzw. Beitragsservice und Rundfunkgebühren bzw. Rundfunkbeitrag:
\ Stellungnahme zum Entwurf des 15. Rundfunkänderungsstaatsvertrages
\ Einmaliger Meldedatenabgleich für den neuen Rundfunkbeitrag
\ Protokollierung lesender Zugriffe auf Teilnehmerdaten
\ Einrichtung eines Datenschutzausschusses bei der GEZ
\ Bericht aus der AG Rundfunkgebühren

Erfahrungsaustausch zu spezifischen Fragen und konkreten Fällen in der Praxis:
\ Berichte aus dem IT-Sicherheitsgremium der ARD
\ Berichte aus dem AK Medien
\ Datenschutzprüfung beim Beihilfeberechnungszentrum bbz
\ Datenschutz und Datensicherheit im Web 2.0 der Landesrundfunkanstalten
\ Like-it-Button/Fanpages bei Facebook
\ Leitfaden Social Media Guidelines
\ Registrierungsverfahren für mein!KI.KA
\ Erhebung von Daten von Kindern bei Onlinegewinnspielen
\ Berichte von Veranstaltungen
\ Anforderungen an den Datenschutz bei hybriden Endgeräten (HbbTV)

2. Vertretung des AK DSB in der Europäischen Datenschutzgruppe nach Art. 29 der EG-Datenschutzrichtlinie

Nach Art. 29 Abs. 2 der EU-Datenschutzrichtlinie ist eine Europäische Datenschutzgruppe, die aus Vertreterinnen und Vertretern der einzelnen Mitgliedstaaten der EU besteht, eingesetzt. Sie soll zu einer einheitlichen Anwendung der Datenschutzrichtlinie in den EU-Staaten beitragen und generell die EU-Kommission beraten. Die stellvertretende Datenschutzbeauftragte des NDR, Frau Koch-Lange, vertrat seit Mitte 2008 bis in den Berichtszeitraum hinein den AK DSB in dieser Arbeitsgruppe.

3. 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 eine Vertreterin/ Vertreter des AK DSB zu den Sitzungen des AK Medien eingeladen. Im Berichtszeitraum wurden beispielsweise Fragen zum neuen Beitragsstaatsvertrag, die Zusammenarbeit zwischen GEZ und Creditreform, die Verarbeitung personenbezogener Daten bei der Nutzung der Tagesschau-App sowie die Ermittlungsbefugnisse der Polizei in sozialen Netzwerken gemeinsam erörtert.

Wie bereits erwähnt wurde im Gegenzug die Vorsitzende des AK Medien, die Datenschutzbeauftragte des Landes Brandenburg, Frau Hartge, bei gemeinsam interessierenden Themen zu einem Teil der Sitzung des AK DSB eingeladen. Für den AK DSB übernimmt die Datenschutzbeauftragte des RBB, Frau Naujock, die Vertretung im AK Medien.

4. Arbeitskreis IT-Sicherheitsgremium

Herr 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 dieses Gremiums.

Anhang: 1. Beitrag des AK DSB zur Positionierung der Rundfunkanstalten zum Vorhaben der EU-Kommission für ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 23. März 2011

I. ALLGEMEINE ANMERKUNGEN

Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) legt nachfolgend zu dem Vorhaben der EU-Kommission für ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ – wie es die EU-Kommission insbesondere in ihrer Mitteilung vom 4. November 2010 (KOM (2010) 609 endg.) beschrieben hat – seine Überlegungen dar.

Ein Gesamtkonzept für den Datenschutz erfasst die wesentlichen Rahmenbedingungen für eine datenschutzrechtliche Regulierung sowohl auf europäischer sowie mitgliedstaatlicher Ebene und bestimmt auch Verhältnis und Gewichtung zu anderen Themen. Das Konzept sollte auch kongruent zu Entwicklungen sein, wie sie etwa im Rahmen der Aktualisierung der Datenschutzkonvention 108 des Europarates erörtert werden. Für den Rundfunk ist neben dem Datenschutz seiner Rezipientinnen und Rezipienten und deren Recht auf anonymen Informationszugang die Wahrung des Medienprivilegs (einschließlich Satire- und Kunstfreiheit sowie Meinungsäußerungsfreiheit; Schutz von Recherche und Informanten einschließlich technischer Daten) von besonderem Interesse. Das setzt unabhängige Datenschutzkontrollstellen, die frei von staatlicher Einflussnahme sind, voraus. Als Kontrollstellen im Sinne von Art. 28 EU-Datenschutzrichtlinie haben die im AK DSB zusammengeschlossenen Rundfunkdatenschutzbeauftragten ein besonderes Interesse an der Erneuerung und Verbesserung des Gesamtkonzepts für den Datenschutz in der Europäischen Union.

Zu einem Gesamtkonzept für den Datenschutz in der Europäischen Union und den von der EU-Kommission in ihrer Mitteilung vom 04.11.2010 beschriebenen fünf Hauptzielen eines solchen Konzepts (Stärkung der Rechte des Einzelnen, Stärkung der Binnenmarktdimension, Änderung der Datenschutzvorschriften in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, Umgang mit der globalen Dimension des Datenschutzes, Verstärkung des institutionellen Rahmens für eine bessere Durchsetzung der Datenschutzvorschriften) nimmt der AK DSB wie folgt Stellung:

II. DATENSCHUTZ UND FREIHEIT DER MEDIEN

Mit dem Lissabon-Vertrag wurde die Europäische Grundrechtecharta verbindlich. Sie erhielt damit den Rang von Primärrecht und die Europäische Union und die Mitgliedstaaten sind folglich bei der Durchführung von europäischem Recht an die Grundrechte der Grundrechtecharta gebunden. Zu den gleichermaßen schützenswerten und miteinander in Ausgleich zu bringenden Grundfreiheiten gehören gemäß Art. 8 der Charta der Schutz personenbezogener Daten sowie gemäß Art. 11 der Charta die Freiheit der Meinungsäußerung, die Informationsfreiheit und die Freiheit der Medien. Nach Art. 51 der Charta und Art. 6. EUV werden dabei die Zuständigkeiten der EU durch die Charta nicht verändert und nicht erweitert.

Mit dem neu geschaffenen Art. 16 AEUV, der in Fortentwicklung der früheren Datenschutzbestimmung in Art. 286 EG-Vertrag Art. 8 der Grundrechtecharta wiederholt, besteht für die Europäische Union eine Rechtsgrundlage für den Erlass datenschutzrechtlicher Vorschriften. Dabei ist aber auch der Schutz der in Art. 11 der Charta genannten Grundrechte zu beachten. Demzufolge sind der Datenschutz nach Art. 8 der Grundrechtecharta und die Meinungsäußerung- und Informationsfreiheit nach Art. 11 der Grundrechtecharta miteinander in Ausgleich zu bringen, und es muss beiden Grundrechten das größte Maß an Wirksamkeit zugesichert werden.

Der Einklang von Datenschutz und Meinungs- und Medienfreiheit ist Gegenstand von Art. 9 der bisherigen Datenschutzrichtlinie (vergleiche EuGH Rs. C-73/07 – Satakunnan Markkinapörssi und Satamedia; vergleiche zum Medienprivileg auch BGH, Urteil vom 15. Dezember 2009, VI ZR 228/08 – Sedlmayr). Zu einem tragfähigen Gesamtkonzept für den Datenschutz in der Europäischen Union gehörten die Beibehaltung und Absicherung dieses in Art. 9 EU-Datenschutzrichtlinie geregelten Medienprivilegs als Aufgabe der Mitgliedstaaten (siehe dazu auch Urteile des EuGH vom 20. Mai 2003 – Rs. C-465/00 – und vom 6. November 2003 – RS.C-101.01). Durch Art. 167 AEUV bleibt der Rundfunk, der zum Bereich der Kultur gehört, der Regelungskompetenz der Mitgliedstaaten vorbehalten. Die Ziele der stärkeren Harmonisierung der Datenschutzvorschriften innerhalb der EU und der Stärkung der Rechte des Einzelnen dürfen nicht zu einer Einschränkung des Regelungsgehalts von Art. 9 der derzeitigen Datenschutzrichtlinie führen.

Das Medienprivileg, das einen Ausgleich zwischen dem Datenschutz und der Meinungs- und Informationsfreiheit schafft, muss sogar noch stärker als bislang abgesichert werden. Für die Rundfunkanstalten ist es unerlässlich, umfangreiche Informationen zu sammeln, zu verarbeiten und zu veröffentlichen. Nur so können sie ihrer Aufgabe, die Bürgerinnen und Bürger mit umfassenden Informationen über Politik, Kultur, Zeitgeschehen und aktuelle Entwicklungen zu versorgen, die für den Meinungsbildungsprozess in einer demokratischen Gesellschaft unabdingbar ist, überhaupt erfüllen. Dazu muss es den Rundfunkanstalten aber möglich sein, ohne Behinderung durch entgegenstehende Vorschriften auch personenbezogene Daten zu erheben und zu verarbeiten.

Um die Rechte des Einzelnen auf Datenschutz zu wahren, gelten für den Rundfunk in Deutschland spezielle Vorschriften, die den Datenschutz sicherstellen. Während für den privaten Rundfunk § 47 Abs. 1 des Rundfunkstaatsvertrages diesbezügliche Sondervorschriften vorsieht, sind für den öffentlich-rechtlichen Rundfunk Datenschutzvorschriften in den Landesdatenschutzgesetzen beziehungsweise in den für die einzelnen Anstalten geltenden Vorschriften vorhanden. Dem Betroffenen einer Sendung wird ein Auskunftsrecht zuerkannt, das sich grundsätzlich auf alle zu seiner Person gespeicherten Daten bezieht. Dieses Recht kann lediglich beschränkt werden, sofern durch das Auskunftsrecht die journalistischen Aufgaben der Rundfunkanstalt beeinträchtigt oder Rückschlüsse auf Mitarbeiter oder Informanten ermöglicht werden würden (vergleiche zum Beispiel § 42 NDR Staatsvertrag, § 37 rbb-Staatsvertrag). Weiterhin stehen dem Betroffenen bei einer unrechtmäßigen journalistischen Berichterstattung zivilrechtliche Ansprüche wie Widerrufs-, Unterlassungs-, Gegendarstellungs- oder Schadensersatzansprüche zu. Auch eine gefestigte journalistische Ethik sowie der jeweilige Datenschutzbeauftragte der öffentlich-rechtlichen Rundfunkanstalt tragen zum Schutz der informelle Selbstbestimmung des Einzelnen im öffentlich-rechtlichen Rundfunk in Deutschland bei.

Eine Einschränkung des Medienprivilegs könnte beispielsweise dazu führen, dass aktuelle Themen nicht mehr zeitnah publiziert werden könnten, wenn zuvor erst die datenschutzrechtlichen Aspekte geprüft werden müssten. Auch die Sammlung von Daten über Personen, um diese etwa für einen späteren Zeitpunkt oder für einen Bericht über ein bestimmtes Ereignis verwenden zu können, wäre nicht möglich. Ebenso ist es für Reportagen und Dokumentationen unerlässlich, über umfangreiches Datenmaterial verfügen zu können. Bei Themen, bei denen ein öffentliches Informations- und Berichterstattungsinteresse besteht, Behörden im Umgang mit Personen zu zeigen (zum Beispiel bei Straßenverkehrskontrollen, Ausübung von Betreuungsrechten, Sozialamtstätigkeiten), muss es Polizei-, Sozial- oder sonstigen Behörden gestattet sein, die Begleitung ihrer Tätigkeiten und Amtshandlungen durch ein Autorenteam (auch mit Kamera oder sonstigen Bildmedien) zu ermöglichen. Bestünde bei diesen – gelegentlich unter dem Stichwort Reality TV behandelten – Themen eine derartige Gestattungsmöglichkeit nicht, wären eine Recherche und gegebenenfalls eine Berichterstattung über wichtige Themen von öffentlichem Interesse nicht möglich. Hierin läge eine unverhältnismäßige Einschränkung des Medienprivilegs. Stattdessen sind die Rechte betroffener Personen weniger durch den Datenschutz, sondern vielmehr im Rahmen des Medienprivilegs durch medienrechtliche und persönlichkeitsrechtliche Grundsätze zu wahren: So werden berechtigte Anonymisierungsinteressen von Personen in einer Berichterstattung durch Unkenntlichmachung berücksichtigt.

Daneben ist es unentbehrlich, Informationen zu archivieren, um bei Bedarf aktuelle Meldungen mit Hintergrundmaterial zu vervollständigen. Denn nur auf diese Weise ist es denkbar, umfassend informieren und berichten zu können. Auch muss es möglich sein, den Schutz der Informatinnen und Informanten weiterhin zu garantieren und das Redaktionsgeheimnis zu wahren, um die Möglichkeit der kritischen Berichterstattung nicht zu gefährden.

Zur redaktionellen Tätigkeit gehören Diskretion über Inhalt und Umfang von Informationen, Informanten- und Rechercheschutz sowie die zur Umsetzung dieser Anforderungen notwendigen technischen Vorkehrungen zur Gewährleistung auch der Datensicherheit. Nur die Gewährleistung dieser Schutzziele des Medienprivilegs ermöglicht, dass Datenschutz und Medienfreiheit thematisch oft Hand in Hand gehen. Vergleiche dazu zum Beispiel folgende Berichte:

\ http://www.ndr.de/regional/hamburg/sparkasse129.html – 200.000 Euro Bußgeld für die Haspa
\ http://www.ndr.de/regional/datenpanneawd106.html – AWD bestreitet neuen Verstoß gegen Datenschutz
\ http://www.ndr.de/regional/famila100.html – Umstrittene Einwilligungserklärungen an der Supermarktkasse
\ http://www.ndr.de/regional/ihrplatz108.html – Drogeriekette überwacht Mitarbeiter und Kunden

Die berechtigte datenschutzrechtliche Diskussion um neue Angebote der sogenannten „mapping industry" darf im Übrigen die bislang unstreitige Rechtmäßigkeit von Aufnahmen vom öffentlichen Grund aus zu Berichterstattungszwecken nicht beeinträchtigen.

Soweit die Mitteilung auf Seite 6, auch unter Fußnote 14, auf die Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 (1 BvR 370/07) Bezug nimmt, mit der Vorschriften im Verfassungsschutzgesetz Nordrhein-Westfalen zur Onlinedurchsuchung und zur Aufklärung des Internets für verfassungswidrig erklärt worden sind, erscheint die Einführung einer Regelung auf EU-Ebene nicht erforderlich. Soweit es um den heimlichen Zugriff auf informationstechnische Systeme im Rahmen einer Onlinedurchsuchung geht, ist im Übrigen auf mitgliedstaatlicher Ebene sicherzustellen, dass der erhöhte Schutzbedarf journalistischer Recherchen hierdurch nicht umgangen oder gar ausgehöhlt werden kann.

Im Falle einer Anpassung der Datenschutzvorschriften in den Bereichen der polizeilichen und justiziellen Zusammenarbeit bedarf es ebenfalls der Wahrung des Medienprivilegs einschließlich der Wahrung des journalistisch-redaktionellen Quellenschutzes. Hierzu gehören auch die Sicherstellung der vertraulichen Kommunikation durch Medienvertreterinnen und -vertreter und die Gewährleistung des Auskunfts- und Zeugnisverweigerungsrechts.

Schließlich sollte ein Gesamtkonzept für den Datenschutz in der EU auch die EU-Richtlinie zur Vorratsdatenspeicherung auf den Prüfstand stellen und eine vorsorgliche Speicherung von Telekommunikationsverkehrsdaten nicht zulassen, soweit Erforderlichkeit und Verhältnismäßigkeit derartiger Speicherungen – etwa auch bezogen auf bestimmte Berufsgruppen wie Journalistinnen und Journalisten – nicht nachgewiesen sind.

III. BINNENMARKTDIMENSION UND GLOBALE DIMENSION DES DATENSCHUTZES

Während bezüglich des Medienprivilegs kein Bedarf für eine weitere Harmonisierung auf EU-Ebene ersichtlich ist, ist der von der EU-Kommission geschilderte Bedarf für eine weitere Harmonisierung in einzelnen von der Datenschutzrichtlinie geregelten Bereichen – vor allem vor dem Hintergrund der globalen Dimension des Datenschutzes – durchaus nachvollziehbar. Zu diesem Zweck erscheint es ausreichend, die bestehende Datenschutzrichtlinie zu novellieren und zu modernisieren. Anlass für eine vollständige Harmonisierung und gegebenenfalls eine Ablösung der Richtlinie durch das Rechtsinstrument einer Verordnung besteht dagegen nicht.

Wünschenswert wäre auch eine Klärung zu anderen Querschnittsmaterien – wie etwa dem Verhältnis von Datenschutz und Urheberrecht (etwa bezogen auf die Verfolgung und Ahndung von Internetpiraterie).

Im Sinne einer Kohärenz des Rechtsrahmens erscheint etwa eine Zusammenführung von Datenschutzrichtlinie und E-Privacy-Richtlinie (Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischenKommunikation) gangbar.

In jedem Falle wird eine Beibehaltung des bisherigen technologieneutralen Ansatzes befürwortet. Dabei darf die weiter fortschreitende Digitalisierung nicht zu einem geringeren Schutz des Rechts auf Schutz personenbezogener Daten führen. Im Gegenteil muss der technologieneutrale Ansatz auch neue Entwicklungen wie zum Beipsiel „cloud computing" erfassen und ihnen gerecht werden können. Dabei kann die Einführung eines Rechenschaftsprinzips der nachhaltigen Verantwortlichkeit („accountability") hilfreich sein.

Ebenso sollte die Verbesserung des Datenschutzes im Internet auch auf EU-Ebene befördert werden. Der Bildung personenbezogener Profile außerhalb journalistischer Zwecke aus Datenquellen unterschiedlichster Herkunft und unabhängig vom ursprünglichen Erhebungszweck, insbesondere zu Werbezwecken, sollte ohne hierauf bezogene ausdrückliche Einwilligung der Betroffenen im Sinne sogenannter Opt-in-Lösungen verboten bleiben. Mit Blick auf Angebote wie z.B. Tracking von Online-Nutzungen, verhaltensbezogene Onlinewerbung, Soziale Online-Netzwerke, aber auch sonstige Profilbildungen (zum Beispiel bezüglich Kunden- oder Bankkarten) ist es wünschenswert, dass außerhalb der EU ansässige Anbieter im Falle einer Betätigung innerhalb der EU an das Niveau der Datenschutzstandards der EU gebunden sind.

Die Untersuchung von Möglichkeiten für eine Vereinfachung oder gegebenenfalls eine Ersetzung der Melderegelungen sowie für eine Präzisierung der Vorschriften über das anwendbare Recht werden begrüßt.

Die Rundfunkdatenschutzbeauftragten achten bereits gegenwärtig auf die strikte Einhaltung der Grundsätze der Datenvermeidung und Datensparsamkeit. Hierzu gehört, dass neue Systeme von vornherein datenschutzgerecht geplant werden. Dies entspricht dem Konzept „Privacy by design", dessen Erfassung im Zuge der Novellierung der Datenschutzrichtlinie sinnvoll erscheint.

IV. STÄRKUNG DER RECHTE DES EINZELNEN

Der AK DSB unterstützt das Vorhaben einer Stärkung der Betroffenenrechte vor allem in Bezug auf die Onlineumgebung.

Dabei ist Transparenz eine Grundvoraussetzung dafür, dass der Einzelne die Kontrolle über seine personenbezogenen Daten hat und ein wirksamer Datenschutz gewährleistet werden kann. Dies gilt insbesondere für den Onlinebereich, in dem für den Betroffenen oft nicht ersichtlich und angesichts der technisch komplexen Hintergründe auch schwer nachvollziehbar ist, ob, von wem und zu welchem Zweck seine Daten erfasst werden.

Daher begrüßt der AK DSB die Einführung eines entsprechenden Transparenzgrundsatzes, in dem festgelegt wird, dass die Betroffenen von den für die Verarbeitung Verantwortlichen umfassend, klar und in transparenter Weise darüber informiert werden, wie, von wem und aus welchem Grund ihre Daten erfasst und verarbeitet werden, wie lange sie aufbewahrt werden und ob sie Zugriff auf ihre Daten haben und die Berichtigung oder Löschung der Daten verlangen können.

Die Entwicklung eines entsprechend EU-weit standardisierten Datenschutzhinweises als unverbindliches Muster, an dem sich die für die Datenverarbeitung Verantwortlichen orientieren können, wird hierbei vom AK DSB als hilfreich angesehen. Für ihre Onlineangebote halten die öffentlich-rechtlichen Rundfunkanstalten entsprechende umfassende Datenschutzhinweise vor (vergleiche zum Beispiel http://www.br-online.de/unternehmen/impressum/impressum-DID1202228323 29/impressum-datenschutzerklaerung-unternehmen-ID1198252389347.xml).

Der AK DSB teilt die Auffassung der Kommission, dass Kinder einen besonderen Schutz bei der Verarbeitung ihrer personenbezogenen Daten genießen müssen, da sie sich in der Regel der Risiken, Folgen, Garantien und Rechte bei der Verarbeitung personenbezogener Daten weniger bewusst sind. Daher erachten es die öffentlich-rechtlichen Rundfunkanstalten als wesentlich, gerade Kinder altersgerecht über Datenschutz aufzuklären. So werden zum Beispiel in dem an Minderjährige adressierten Onlineangebot „tivi.de“ des ZDF sowie in dem Onlineangebot des Kinderkanals von ARD und ZDF „kika.de“ die Datenschutzerklärungen für die Eltern zusätzlich von speziellen kindgerechten Datenschutzerklärungen begleitet.

- http://www.kika.de/service/datenschutz/index.shtml (Datenschutzhinweis speziell für Kinder) und http://www.kika.de/kika/eltern/datenschutz/index.shtml (Datenschutzhinweise für die Eltern)
- http://www.tivi.de/tivi/sicherheit/artikel/20137/index.html (Datenschutzhinweis speziell für Kinder)
- Hinweise zum Datenschutz auf dem Angebot Kinderinsel auf BR-online http://www.br-online.de/kinder/treffen-finden/wir/datenschutz/ (für Kinder) und http://www.br-online.de/kinder/treffen-finden/wir/erwachsene/ (für Eltern)

Der AK DSB ist der Auffassung, dass es für einen effektiven Selbstdatenschutz wichtig ist, dass Personen informiert werden, wenn ihre Daten versehentlich oder unrechtmäßig gelöscht oder geändert wurden, wenn sie verloren gegangen sind oder wenn Unbefugte darauf zugegriffen oder sie weitergegeben haben.

Mit der Novellierung des deutschen Bundesdatenschutzgesetzes (BDSG) wurde zum 1. September 2009 in § 42a BDSG eine gesetzliche Anzeigepflicht eingeführt, wonach Unternehmen die zuständige Datenschutzbehörde und die Betroffenen informieren müssen, falls besonders sensible personenbezogener Daten, einer beruflichen Verschwiegenheitspflicht unterliegende Daten, Bank- und Kreditkartendaten oder Daten bezüglich krimineller Aktivitäten verloren gehen, unrechtmäßig übermittelt werden oder kompromittiert werden. Eine entsprechende Anzeigepflicht ist aus Sicht des AK DSB sinnvoll und ausreichend, allerdings unter Berücksichtigung der besonderen Stellung der öffentlich-rechtlichen Rundfunkanstalten, insbesondere auch der Unabhängigkeit von staatlichen Aufsichtsbehörden.

Bessere Kontrolle des Betroffenen über seine Daten
Die Rundfunkdatenschutzbeauftragten achten bereits gegenwärtig auf die strikte Einhaltung der Grundsätze der Datenvermeidung und Datensparsamkeit. Hierzu gehört, dass neue Systeme von vornherein datenschutzgerecht geplant werden. Dies entspricht dem Konzept „eines Privacy by design“, dessen Erfassung im Zuge der Novellierung der Datenschutzrichtlinie sinnvoll erscheint. In diesem Zusammenhang ist darauf hinzuweisen, dass im Zuge der Novellierung des Bundesdatenschutzgesetzes in der Neufassung des § 3a BDGS erstmals für alle Erhebungen, Verarbeitungen und Nutzungen die Pflicht zur Datensparsamkeit und Anonymisierung gesetzlich festgelegt worden ist. So müssen alle Daten anonymisiert werden, wenn nicht hierzu ein unverhältnismäßig hoher Aufwand nötig ist und dies der Einsatzzweck der Daten zulässt. Zudem muss bei der Auswahl und Herstellung von Softwareprodukten darauf geachtet werden, dass diese so wenig personenbezogene Daten benutzen wie möglich.

Was die öffentlich-rechtlichen Rundfunkanstalten betrifft, so ist die Angabe spezieller persönlicher Daten für den Zugang zu den Inhalten der frei empfangbaren Programmangebote der öffentlich-rechtlichen Rundfunkanstalten grundsätzlich nicht notwendig. Bei besonderen Angeboten im Onlinebereich der Rundfunkanstalten – wie zum Beispiel sozialen Netzwerken oder andere Web. 2.0-Elementen oder Communities – können solche Daten für den Zugang zur „Plattform“ bzw. dem Angebot abgefragt werden, die für die Nutzung des Angebots erforderlich sind. Mit Blick auf neue Anwendungen wie beziehungsweise das hybride Fernsehen HbbTV wird ebenfalls darauf zu achten sein, dass die Möglichkeit des freien Zugangs zu den öffentlich-rechtlichen Angeboten gewährleistet bleibt und der Zugang nicht von Registrierungen, Datenabfragen und Datenverarbeitungsmöglichkeiten von Geräteherstellern und/oder Providern abhängig gemacht wird, die für die Nutzung der Angebote gar nicht erforderlich sind. Eine systemseitig angelegte Voreinstellung für ein Tracking der Nutzungen zum Zwecke verhaltensbezogener Werbung muss ohne Opt-in der Rezipientinnen und Rezipienten unbedingt unterbleiben.

Im Hinblick auf die angedachte Einführung eines „Rechts auf Vergessenwerden“ sind aus Sicht des AK DSB die Bedeutung

beziehungsweiseder Mehrwert sowie die Reichweite und die technische Umsetzung eines solchen Rechts – auch im Hinblick auf das bereits bestehenden Recht auf Löschung von Daten – noch nicht ausreichend klar definiert. Die Kommission hat bei ihren Überlegungen offenbar vor allem die sozialen Onlinenetzwerke im Fokus, auf denen eine Vielzahl persönlicher Daten gespeichert sind.

Die öffentlich-rechtlichen Rundfunkanstalten entlassen Nutzerinnen und Nutzer unkompliziert aus ihren Netzwerken und anderen Social-Media-Angeboten. Hier gilt der Grundsatz der Löschung von Daten, die nicht mehr benötigt werden oder deren Userinnen und User sich zum Beispiel bei einem Forum oder Ähnlichem abgemeldet haben. Allgemein gilt für die öffentlich-rechtlichen Onlineangebote zudem ein detailliertes und umfassendes Verweildauerkonzept. Außerhalb von Archiven tritt danach das „Vergessen" in den deutschen öffentlich-rechtlichen Telemedien nach spätestens fünf Jahren ein.

Sollte ein solches „Recht auf Vergessenwerden" eingeführt werden, müsste zur Wahrung des Medienprivilegs in jedem Fall differenziert werden zwischen den Informationen, die auch weiterhin in den öffentlich-rechtlichen Archiven erhalten bleiben müssen, sowie dem generellen Recht des Einzelnen, die Kontrolle über seine eigenen persönlichen Daten zu haben. Auch eine Begrenzung des „Rechts auf Vergessenwerden" speziell für die sozialen Onlinenetzwerke wäre zu prüfen.

Auch bei der Frage, ob ein neues Recht für von der Datenverarbeitung Betroffene eingeführt wird, in dem die „Datenübertragbarkeit" sichergestellt wird, scheint die Kommission vor allem wieder die sozialen Onlinenetzwerke im Blick zu haben. Auch hier stellt sich die Frage, inwieweit eine solche Datenübertragbarkeit technisch für den Betroffenen überhaupt möglich ist, auch ohne von dem für die Verarbeitung Verantwortlichen daran gehindert zu werden.

Bewusstsein und Aufklärung fördern
Die Kommission erkennt zurecht, dass es notwendig ist, die Allgemeinheit, insbesondere junge Leute, besser über die Risiken der Verarbeitung personenbezogener Daten aufzuklären und besser im richtigen Umgang mit den eigenen Daten zu schulen.

Die öffentlich-rechtlichen Rundfunkanstalten nehmen diese Aufgabe im Rahmen ihres Informations-, Bildungs- und Beratungsauftrags wahr. Das Thema Datenschutz ist regelmäßig Gegenstand der Berichterstattung in Hörfunk, Fernsehen und online.

Speziell für den Bereich des Internets haben die Rundfunkanstalten zudem den Auftrag, mit ihren Onlineangeboten allen Bevölkerungsgruppen die Teilhabe an der Informationsgesellschaft zu ermöglichen sowie die technische und inhaltliche Medienkompetenz aller Generationen und von Minderheiten zu fördern (vergleiche § 11d Abs. 3 RfStV). Daher gibt es in den Telemedien der ARD zahlreiche Inhalte zum Thema verantwortungsvoller Umgang mit neuen Medien, Social Networks und Datenschutz im Internet. Vergleiche zum Beispiel folgende Seiten:

\ http://www.ard.de/ratgeber/multimedia/-/id=13302/9pbsn3/index.html (Tipps und Beratung zum Thema Multimedia und Datenschutz)
\http://www.br-online.de/ratgeber/familie/safer-internet-DID1263803604915/index.xml (Dossier zum Thema „Safer Internet")
\ http://www.wdr.de/tv/monitor/dossiers/datenschutz.php5 (Dossier zum Datenschutz)
\ http://www.rbb-online.de/ratgeber/dossiers/social_media/sicher_unterwegs_im_netz.html (Ratgeber „Sicher unterwegs im Internet)
\ http://www.rbb-online.de/ratgeber/dossiers/social_media/soziale_netzwerke_wissenswertes.html (Ratgeber „Soziale Netzwerke")
\ http://www.rbb-online.de/ratgeber/dossiers/social_media/facebook_datenschutz_einsteiger.html (Ratgeber „Privacy-Einstellungen bei Facebook")

Kinder und Jugendliche werden von den öffentlich-rechtlichen Rundfunkanstalten in ihren Onlineangeboten altersgerecht über Datenschutz aufgeklärt (siehe Seite 6 f.).

Im Sinne der Förderung der Medienkompetenz für alle Bevölkerungsgruppen hat sich die ARD in ihren Leitlinien für 2011 und 2012 verpflichtet, ihr redaktionell-journalistisches Angebot zum Thema neue Medien und hier insbesondere zu Social Networks und Datenschutz noch weiter zu verbessern. Ziel ist es, die vielfältigen diesbezüglichen Inhalte zum Thema Medienkompetenz in der ARD zu bündeln, durch die Arbeit der Experten in den Onlineredaktionen zu ergänzen und einen thematischen Schwerpunkt zu etablieren, an dem verlässlich und stets aktuell die Informationen von den Nutzern gefunden werden können. Auch das ZDF wird sich in seinem publizistischen Angebot für eine kontinuierliche Weiterentwicklung des Selbstdatenschutzes einsetzen.

Stärkung des Prinzips der informierten Einwilligung
Der AK DSB begrüßt das Vorhaben der Kommission, zu prüfen, ob und wie das Prinzip der informierten Einwilligung präzisiert und gestärkt werden kann. Insbesondere erscheinen in diesem Zusammenhang ergänzende Regelungen für die Onlineumgebung sinnvoll: So sollten ausdrückliche Einwilligungen in Form von sogenannter Opt-in-Klauseln für den Bereich der verhaltensorientierten Internetwerbung eingeführt werden.

Die Bildung personenbezogener Profile aus Datenquellen unterschiedlichster Herkunft und unabhängig vom ursprünglichen Erhebungszweck, außerhalb des journalistisch-redaktionellen Bereichs, insbesondere zu Werbezwecken, sollte ohne hierauf bezogene ausdrückliche Einwilligung der Betroffenen ebenfalls im Sinne sogenannter Opt-in-Lösungen verboten bleiben. Die jeweiligen Einstellungen des Internetbrowsers beziehungsweise andere Opt-out-Möglichkeiten erscheinen nicht ausreichend, um von der geforderten Einwilligung der Nutzerin/des Nutzers ausgehen zu können.

V. VERSTÄRKTER INSTITUTIONELLER RAHMEN FÜR EINE BESSERE DURCHSETZUNG DER DATENSCHUTZ-VORSCHRIFTEN

Für die Durchsetzung von Datenschutzvorschriften ist die Unabhängigkeit der Datenschutzaufsichtsbehörden von wesentlicher Bedeutung. Der EuGH hat dies in seinem Urteil vom 9. März 2010 (Kommission gegen Deutschland, Rechtssache C-518/07) mit Blick auf die Unabhängigkeit der für den privaten Bereich zuständigen datenschutzrechtlichen Kontrollstellen von staatlicher Aufsicht bestätigt.

Dieses Konzept passt zu der Art und Weise der Organisation des öffentlich-rechtlichen Rundfunks, der einerseits frei von staatlicher Einflussnahme und Aufsicht organisiert sein muss und andererseits gemäß dem sogenannten Amsterdamer Protokoll über den öffentlich-rechtlichen Rundfunk in den Kompetenzbereich der Mitgliedstaaten gehört. Insofern lässt sich aus den Ausführungen des EuGH zur Unabhängigkeit der datenschutzrechtlichen Kontrollstellen von staatlichen Stellen und politischer Einflussnahme eine Bestätigung des Konzepts ableiten, die Rundfunkdatenschutzbeauftragten als Kontrollstellen für den gesamten Tätigkeitsbereich der jeweiligen öffentlich-rechtlichen Rundfunkanstalt im Sinne von Artikel 28 Abs. 1 EU-Datenschutzrichtlinie beizubehalten beziehungsweise einzurichten, die in der Ausübung ihres Amtes völlig unabhängig und nur dem Gesetz unterworfen sind.

Dem entsprechen die gegenwärtigen landesgesetzlichen Regelungen in der Bundesrepublik Deutschland auf der Grundlage der EU-Datenschutzrichtlinie auch, indem die Beauftragten für den Datenschutz von den Aufsichtsgremien bestellt werden und auch lediglich einer beschränkten Dienstaufsicht durch die Aufsichtsgremien unterstehen.

Die Rundfunkdatenschutzbeauftragten unterstützen Bemühungen, die Effizienz der Datenschutzaufsicht bei den öffentlich-rechtlichen Rundfunkanstalten durch unabhängige Rundfunkdatenschutzbeauftragte, die frei von staatlicher Einflussnahme agieren, weiter zu verbessern und damit dem Grundrecht auf Datenschutz nach Art. 8 des Vertrages von Lissabon noch besser Rechnung zu tragen.

2. Social Media Leitfaden

Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR – 26. April 2012

A. Vorbemerkungen

Mit diesem Leitfaden wird der Leitfaden des AK DSB zu Datenschutz und Datensicherheit in sozialen Netzwerken vom Mai 2009 aktualisiert und ergänzt.

Soziale Medienangebote (Social Media) dienen dazu, sich mithilfe digitaler Medien und Technologien untereinander auszutauschen. Zu diesem Zweck werden persönliche Daten – auch digitale Fotos und Videos – in aller Welt mehr oder weniger verfügbar gemacht. Zu Social Media gehören interaktive Angebote und Dienste, wie unter anderem Chats, Foren, Blogs und Soziale Netzwerke.

Social-Media-Angebote dominieren zunehmend das Mediennutzungsverhalten in bestimmten Zielgruppen. Daher verwenden auch die öffentlich-rechtlichen Rundfunkanstalten solche Angebote und sind auch selbst Betreiber sozialer Netzwerke, zum Beispiel durch die Hörfunkwellen MeinFritz.de vom rbb, myS-PUTNIK.de vom MDR und myYOU-FM.de vom hr. Diese sozialen Netzwerke ermöglichen es den Nutzerinnen und Nutzern, mit Gleichgesinnten in Kontakt zu treten, sich an dem öffentlichen Meinungsbildungsprozess zu beteiligen und beispielsweise eigene Musik mittels eines entsprechenden Videoclips zu veröffentlichen. Um zusätzliche Zielgruppen zu erreichen, bieten die öffentlich-rechtlichen Rundfunkanstalten inzwischen ihre Angebote auch auf den Plattformen anderer Anbieter – insbesondere auf Facebook und YouTube – an. Diese Entwicklung ist aus Sicht des Datenschutzes kritisch zu betrachten, da die meisten Social-Media-Plattformen Dritter momentan weder den deutschen Datenschutzgesetzen noch den Standards der ARD-Datenschutzbestimmungen genügen.

Aus diesem Grund kommt der Aufklärung der Nutzerinnen und Nutzer über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten eine besondere Bedeutung zu. Das betrifft auch die Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Besondere Schwerpunkte der Aufklärung müssen auch der Umgang mit den Daten Dritter und der Jugendschutz, der unter anderem bei den Angeboten des Kinderkanals von ARD und ZDF eine große Rolle spielt, bilden. Der Vollständigkeit halber sei darauf hingewiesen, dass über die datenschutz- und persönlichkeitsrechtlichen Aspekte hinaus weitere Themen wie zum Beispiel das Urheber-, das Kennzeichen- und Markenrecht sowie das Strafrecht zu beachten sind.

Nachfolgend werden die wesentlichen Anforderungen zu Datenschutz und Datensicherheit bei Social-Media-Angeboten der Rundfunkanstalten dargestellt.

Dieser Leitfaden richtet sich an alle Mitarbeiterinnen und Mitarbeiter, die Social Media im Auftrag der Rundfunkanstalten redaktionell einsetzen beziehungsweise die technischen Voraussetzungen dafür schaffen. Der Leitfaden soll eine erste Orientierung bieten. Er kann den Informationsaustausch zwischen den verantwortlichen Mitarbeiterinnen und Mitarbeitern und den Rundfunkdatenschutzbeauftragten zu Einzelfragen nicht ersetzen.

B. Datenschutz – was ist ganz generell zu beachten?

Datenschutz hat das Ziel, jeden einzelnen Menschen vor den Gefahren beim Umgang mit persönlichen Daten zu schützen. Datenschutz ist daher immer dann zu beachten, wenn personenbezogene Daten abgefragt und verwendet werden.

Unter personenbezogenen Daten versteht man alle Daten, die dazu genutzt werden können, die Identität der Userin/des Users offen zu legen, wie zum Beispiel richtiger Name, Anschrift, Telefonnummer, E-Mail- und IP-Adresse sowie weitere Informationen zum Beispiel. über das Nutzungsverhalten, soweit sie dem Nutzer zugeordnet werden können. Besonders sensible persönliche Daten sind zum Beispiel Angaben über die ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben sowie Daten über Straftaten und Minderjährigendaten.

Für ein datenschutzkonformes Onlineangebot der Rundfunkanstalten gilt ganz generell Folgendes:

\ Eine Erhebung, Speicherung und Nutzung der personenbezogenen Daten einer Nutzerin/eines Nutzers darf grundsätzlich immer nur zu einem bestimmten, jeweils angegebenen Zweck erfolgen. Eine Verwendung der Daten für andere Zwecke ohne Wissen und Einverständnis der Nutzerin/des Nutzers ist unzulässig. Name, Anschrift, E-Mail-Adresse oder Telefonnummer und Ähnliches einer Nutzerin/eines Nutzers dürfen nie pauschal abgefragt und gespeichert werden (Grundsatz der Zweckbindung).
\ Die Nutzerin/Der Nutzer muss genau wissen, für wen/was sie/er welche Daten zur Verfügung stellt (Transparenzgebot) und sie/er muss hierzu seine Einwilligung erklären. Wenn also in den einzelnen Fällen (zum Beispiel bei Gewinnspielen, beim Versand von Newslettern, bei der Anmeldung für Communities et cetera) personenbezogene Informationen eines Nutzers benötigt und gespeichert werden, muss sie/er ausdrücklich und in transparenter Weise auf diesen Sachverhalt aufmerksam gemacht werden. Aus verschiedenen Quellen/Anlässen stammende personenbezogene Daten dürfen nicht zu einem Profil zusammengeführt werden, soweit nicht hierzu die gesondert einzuholende Einwilligung der Nutzerin/des Nutzers erteilt wurde. Nutzer müssen ein Angebot nutzen können, ohne zuvor einer Profilbildung zustimmen zu müssen.
\ Sollen besonders sensible persönliche Daten erhoben, verarbeitet oder genutzt werden, so ist der Nutzer darüber im Zuge seiner Einwilligung gesondert zu unterrichten.
\ Es sollen immer so wenige Pflichtdaten wie möglich, also nur solche Daten, die wirklich erforderlich sind (Prinzip der Datensparsamkeit), abgefragt werden. Beispiel für einen begründeten Ausnahmefall ist die Abfrage von E-Mail-Adressen bei Kommentarfunktionen (nicht öffentlich sichtbar). In der Praxis hat sich gezeigt, dass diese Vorgabe, wenngleich sie de facto keine persönliche Identifizierung ermöglicht, positive Auswirkungen auf das Niveau der Kommentare und den Umgang der Nutzerinnen und Nutzer untereinander hat.
\ Die Nutzerin/Der Nutzer hat das Recht, seine erteilte Einwilligung zur Datenspeicherung mit Wirkung für die Zukunft jederzeit zu widerrufen. Auf dieses Recht muss er ausdrücklich hingewiesen werden.
\ Sobald die personenbezogenen Daten nicht mehr zu dem ursprünglich angegebenen Zweck benötigt werden, müssen sie gelöscht bzw. anonymisiert werden. Das Gleiche gilt im Falle des Widerrufs einer Einwilligungserklärung in die Datenverarbeitung durch die Nutzerin/den Nutzer.
\ Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist durch geeignete technische und organisatorische Maßnahmen so zu gestalten, dass die Daten vor Fehlern, Missbrauch und Zerstörung geschützt sind (Maßnahmen zur Datensicherheit).
\ Der Kontaktweg zur Nutzerbetreuung sollte, ebenso wie das Impressum und der Verweis auf die Beschwerde-/Widerrufsmöglichkeit, für die Nutzerinnen und Nutzer leicht auffindbar sein.

C. Einzelne Datenschutzmaßnahmen auf den Webseiten der Rundfunkanstalten

I. SCHULUNG VON MEDIENKOMPETENZ

Die Angebote der Rundfunkanstalten sollen die Nutzerinnen und Nutzer über die spezielle Problematik von Privatsphäre in Social-Media-Angeboten aufklären. Hierfür sollten zielgruppengeeignete Formen gefunden werden, so zum Beispiel eine Erläuterung der Risiken in Videos.

II. DATENSCHUTZKONFORME GESTALTUNG

1. Beschränkung der Pflichtangaben auf das notwendige Minimum

Der Umfang der von den Nutzerinnen und Nutzern bei der Anmeldung zu Social Media (Registrierung) abzugebenden persönlichen Pflichtangaben ist auf das für die technische Realisierung oder die Erfüllung rechtlicher Auflagen notwendige Minimum zu beschränken (Prinzip der Datensparsamkeit). Dabei hilft die Kontrollfrage: Wozu brauchen wir die Angaben?

Eine anonyme Nutzungsmöglichkeit ist vorab zu prüfen. Eine pseudonyme Nutzung muss möglich sein. Dabei ist der Benutzername nicht mit dem echten Namen identisch, sondern ein frei wählbarer Name. Mit diesem Benutzernamen ist die Teilnehmerin/der Teilnehmer in dem Social-Media-Angebot sichtbar. Es kann aber nicht direkt auf die Person geschlossen werden.

2. „Datenschutzerklärung"/Unterrichtung
Die Rundfunkanstalt hat in ihrem Onlineangebot die Nutzerinnen und Nutzer in einer Datenschutzerklärung über Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten zu informieren. Die Unterrichtungspflicht bezieht sich sowohl auf die Inhaltsdaten (siehe Glossa im Anhang) als auch auf die Bestands- und Nutzungsdaten. Je mehr Daten von den Nutzerinnen und Nutzern erhoben werden und je sensibler die Daten sind, desto ausführlicher muss die Unterrichtung sein. Zudem sollte die Nutzerin/der Nutzer auf das Einwilligungserfordernis und die Möglichkeit des Widerrufs hingewiesen werden. Des Weiteren sollte der Nutzer ausdrücklich auf die Möglichkeit der pseudonymen Nutzung hingewiesen werden. Falls Cookies verwendet werden, ist auch hierüber genau zu informieren (siehe hierzu 12.). Schließlich sollte auch ein Kontakt für datenschutzrechtliche Anfragen und Beschwerden (zum Beispiel der anstaltseigene Datenschutzbeauftragte) genannt werden.

Die Datenschutzerklärung sollte in allgemein verständlicher Form formuliert sein und muss leicht auffindbar und jederzeit abrufbar sein. Eine Datenschutzerklärung muss grundsätzlich für das gesamte Onlineangebot einer Rundfunkanstalt formuliert werden. Für Internetangebote, die sich an Minderjährige richten, ist zusätzlich eine verständliche Form für Kinder wünschenswert (vergleiche III).

Sofern es im Rahmen dieses Onlineangebots Social-Media-Angebote gibt, bieten sich eigene Unterrichtungen (zum Beispiel über einen eigenen Link) zusammen mit den Nutzungsbedingungen speziell zu den Social-Media-Angeboten an. Andernfalls sollten in der allgemeinen Datenschutzerklärung eigene Punkte zu Social Media – insbesondere zu den sozialen Netzwerken – mit ausführlichen Informationen enthalten sein.

3. „Aktive" Einwilligung in die Verarbeitung der personenbezogenen Daten
Für die dauerhafte Speicherung personenbezogener Daten für einen bestimmten Zweck ist eine aktive Einwilligung der informierten Nutzerin/des informierten Nutzers erforderlich. Die Einwilligung muss eindeutig und bewusst erfolgen.

Erreichen lässt sich diese Anforderung zum Beispiel, indem die Nutzerin/der Nutzer ein bestimmtes Feld im Anschluss an die Einwilligungserklärung ankreuzen muss (Checkbox), die ihm anschließend auch dargestellt wird, bevor er die angekreuzte Einwilligungserklärung an die Rundfunkanstalt durch das Anklicken eines Bestätigungsfeldes übersendet. Geeignet ist auch ein Verfahren, bei dem die Rundfunkanstalt der Nutzerin/dem Nutzer die Einwilligungserklärung noch einmal per E-Mail übersendet und sich den Empfang durch das Anklicken eines in der E-Mail abgegebenen Aktivierungslinks bestätigen lässt (sogenanntes Double Opt-in-Verfahren).

Die Einwilligung muss dabei dort eingeholt werden, wo die Daten erhoben oder weitergegeben werden, und gilt nur für den beschriebenen Zweck. Die Einholung einer Einwilligung zu Datenverarbeitungen für sämtliche Social-Media-Angebote ist nur dann möglich, wenn die Nutzerin/der Nutzer hierüber ausdrücklich informiert wird und außerdem weiterhin auch die „einfache" Anmeldung zu einem speziellen Social-Media-Angebot und die dann selbst ausgewählte Teilnahme an den dort angebotenen Einzelaktionen möglich bleibt.

Die Einwilligung muss protokolliert werden und jederzeit für die Nutzerin/den Nutzer abrufbar sein. Es ist ausreichend, wenn die Einwilligung jeweils auf Anfrage zugänglich gemacht wird.

Eine gesonderte Protokollierung kann entfallen, wenn der Zugriff auf die Angebote technisch an eine Einwilligungserklärung gebunden wird, also kein Anmeldeprozess ohne Zustimmung zu den Erklärungen möglich ist. Bei diesem Modell muss die Zustimmung bei Änderung der Bestimmungen zwingend neu eingeholt werden.

Generell sollte im Fall der Änderung der Datenschutzbestimmungen jeweils eine neue Einwilligungserklärung derNutzerinnen und der Nutzer eingeholt werden und auf standardmäßige Änderungsklauseln wie: „Das Recht zu jederzeitigen Änderung an diesen Datenschutzbestimmungen wird vorbehalten ..." verzichtet werden.

4. Einfache Möglichkeit des Widerrufs der Einwilligung
Die Einwilligung muss jederzeit in einfacher Art und Weise von der Nutzerin/vom Nutzer widerrufbar sein. Der Nutzer muss jedenfalls in der Datenschutzerklärung über sein Widerrufsrecht informiert werden.

5. Aktive Freigabe der Daten durch die Nutzerin/den Nutzer
Die Daten, die die Nutzerin/der Nutzer im Rahmen der Anmeldung als Information auf seinem Profil angibt, dürfen zunächst bis auf den Benutzernamen nicht für andere Nutzer sichtbar sein. Die Nutzerin/Der Nutzer muss selbst die Möglichkeit haben und entscheiden können, ob und welche Informationen er für andere Nutzerinnen/Nutzer der Social-Media- Angebote sichtbar macht. Im Rahmen der Einstellungen ist ein differenziertes Berechtigungskonzept nötig (siehe 6.).

6. Differenziertes Berechtigungskonzept bei sozialen Netzwerken
Für ein soziales Netzwerk muss ein differenziertes Berechtigungskonzept festgelegt und umgesetzt werden. Die Nutzerin/Der Nutzer muss dabei selber die Regeln festsetzen können,

\ welche seiner Datenobjekte (Fotos, Freunde, Gästebuch, persönliche Daten)
\ von welcher Gruppe der Zugreifenden – zum Beispiel Freunden – Mitglieden des sozialen Netzwerks – allgemeine Öffentlich-

keit (d.h. auch von Nichtmitgliedern des Sozialen Netzwerks),
\ mit welchen Rechten (zum Beispiel Lesen, Schreiben, Ändern) versehen wird.

Mit einer Art „Ampelsystem“ sollte den Nutzerinnen und Nutzern deutlich angezeigt werden, welcher Kreis auf die jeweiligen Daten aktuell zugreifen kann. Die Ampelmetapher kann der Nutzerin/dem Nutzer bei der Erstellung sowie bei der späteren Ansicht den Berechtigungsstatus seiner Inhalte visualisieren. Der Berechtigungsstatus sollte auch über diese Ampel änderbar sein.

Das Recht zur Selbstbestimmung und der Persönlichkeitsrechtsschutz dürfen nicht durch eine vorhandene Suchfunktion unterlaufen werden. Die Suchfunktion muss also die vom Profilinhaber eingerichteten Zugriffskontrollen berücksichtigen.

Bei der Möglichkeit des schreibenden Zugriffs (zum Beispiel in Form eines Eintrags in das Gästebuch) muss dem Profilinhaber ein Vetorecht eingeräumt werden.

7. Profilbesucherhistorie
Sofern in den Social-Media-Angeboten, insbesondere bei sozialen Netzwerken, auch eine Protokollfunktion vorgesehen ist, mit der für die Mitglieder sichtbar ist, welche Nutzerin/welcher Nutzer welches Profil besucht hat, sollte diese Funktion als Defaulteinstellung nicht aktiviert sein. Die Profilinhaberin/Der Profilinhaber muss selbst entscheiden können, ob er diese Defaulteinstellung ändern will.

8. Begrenzung des Zugriffs auf Social Media von außen
Der Zugriff auf (sensible) personenbezogene Daten der Nutzer durch Nichtmitglieder insbesondere bei Sozialen Netzwerken, von außen, d.h. vom allgemein zugänglichen Teil des Internet auf ein solches Angebot (zum Beispiel über Suchmaschinen) muss technisch ausgeschlossen sein. Auch der Export oder Download persönlicher Daten, die Teil des Profils einer Nutzerin/eines Nutzers sind, durch Dritte müssen – sofern technisch möglich – ausgeschlossen sein.

Es muss sichergestellt sein, dass personenbezogene Daten durch Dritte (zum Beispiel Besucher und Suchmaschinen) nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Dazu zählen auch Profilbilder in selbst betreuten Nutzerprofilen.

9. Daten Dritter
Die Nutzerin/Der Nutzer muss möglichst in einem entsprechenden Textfeld, mindestens aber in den Nutzungsbedingungen, deutlich darauf hingewiesen werden, dass er bei den von ihm eingestellten Inhalten die Persönlichkeitsrechte Dritter zu beachten hat; insbesondere müssen die in seinen Bildern, Videos et cetera. abgebildeten Personen ihre Einwilligung – soweit nach der Rechtslage eine solche nicht entbehrlich ist – zur Veröffentlichung erteilt haben. Für den Fall des widerrechtlichen Einstellens von Daten Dritter sollte sich die Rundfunkanstalt den sofortigen Ausschluss aus ihrem Angebot vorbehalten.

10. Aufgabe der Mitgliedschaft
Es muss eine unkomplizierte Möglichkeit für die Aufgabe der Mitgliedschaft eingerichtet werden. Diese Abmeldefunktion muss auf der Plattform selbst vorhanden und einfach durchzuführen sein. Nicht ausreichend ist die Abmeldemöglichkeit per E-Mail oder Brief an die Rundfunkanstalt.

11. Nach Aufgabe der Mitgliedschaft vollständige Löschung oder Anonymisierung der personenbezogenen Daten
Personenbezogene Daten der Nutzerin/des Nutzers müssen umgehend nach der Aufgabe einer Mitgliedschaft und der entsprechenden Abmeldung in einem technischen Vorgang automatisch gelöscht werden. Diese vollständige Löschung sollte auch die vom Anwender erzeugten Daten außerhalb des Profils erfassen.

Ist eine Löschung technisch nicht möglich, müssen die Daten in jedem Falle anonymisiert werden. Anonymisiert sind die Daten dann, wenn die personenbezogenen Daten derart verändert sind, dass die Informationen einer bestimmten oder bestimmbaren natürlichen Person nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können.

12. Cookies
Die Zulässigkeit der Verwendung von Cookies im konkreten Einzelfall richtet sich nach den allgemeinen datenschutzrechtlichen Grundsätzen, wenn das Cookie personenbezogene Daten (z. B. die IP-Adresse) enthält.

Die Verwendung von Cookies als Nutzungsdaten ist gesetzlich zulässig und bedarf keiner gesonderten Einwilligung, sofern sie für die aktuelle Nutzung der Dienste erforderlich ist. Als Nutzungsdaten sind die Informationen zu betrachten, die während der Nutzung des Onlineangebots, also insbesondere der Interaktion mit dem Anbieter des Social-Media-Angebots, entstehen. Hierbei handelt es sich dann um ein temporäres Cookie (sog. „session cookie“), das nach der Nutzung wieder gelöscht wird.

Das Setzen sog. „permanenter“ Cookies (das heißt von Cookies, die dauerhaft auf der Festplatte des PC abgelegt werden) mit personenbezogenen Daten ist grundsätzlich nur mit Einwilligung der Nutzerin/des Nutzers zulässig. Eine Einwilligung ist dann nicht erforderlich, wenn mithilfe des Cookies anonymisierte oder pseudonymisierte Nutzerprofile für Zwecke der Marktforschung oder zur bedarfsgerechten Gestaltung des Dienstes gebildet werden. Der Bildung eines pseudonymisierten Nutzerprofils muss eine Nutzerin/ein Nutzer jedoch jederzeit widersprechen können.

Unterrichtungspflicht bei Einsatz von Cookies
Die Nutzerin/Der Nutzer muss über die Art, den Umfang und den Zweck des Einsatzes eines Cookies in allgemein verständlicher Form unterrichtet werden. Falls das Cookie die Erhebung oder Verwendung personenbezogener beziehungsweise -beziehbarer Daten vorbereitet, hat die Information über den Einsatz eines Cookies „zu Beginn“ des Einsatzes zu erfolgen. Der Hinweis muss vor dem Einsatz, also vor dem „Ablegen“ des Cookie, gegeben

werden. Praktisch muss der Hinweis so rechtzeitig erfolgen, dass die/der Betroffene die spätere Identifikation noch verhindern kann. Die Nutzerin/Der Nutzer muss dabei klare und ausführliche Informationen über die Verwendung/den Zweck, den Inhalt und das Verfallsdatum des Cookie erhalten und in die Lage versetzt werden, Permanent-Cookies auch ablehnen zu können (üblicherweise dadurch, dass die Nutzerin/der Nutzer darauf hingewiesen wird, dass er durch technische Maßnahmen/Veränderung der Browsereinstellung die Durchführung von Permanent-Cookies abwenden kann).

Die Nutzung des Angebots muss auch ohne Permanent-Cookie weiterhin möglich sein. Darüber und über die Tatsache, dass die Nutzerin/der Nutzer in diesem Fall mit Funktionseinschränkungen rechnen muss, ist er in der Datenschutzerklärung zu informieren. Nicht ausreichend ist der kommentarlose Verweis auf die Einstellung im Browser („Cookie akzeptieren") oder die Zustimmung zu einer Anfrage ohne entsprechende Unterrichtung („xxx will ein Cookie installieren. Sind Sie damit einverstanden?").

13. Speicherung der Protokolldaten

Es sind geeignete technische und organisatorische Maßnahmen zu treffen, um einen sicheren Betrieb und eine sichere Nutzung der Social Media und der gespeicherten persönlichen Daten zu gewährleisten (Näheres dazu siehe E). Die Protokolldaten der Nutzer, die bei der Nutzung der Social-Media-Angebote auf den Onlineseiten der Rundfunkanstalten anfallen (insbesondere die IP-Adresse), dürfen im Regelfall maximal 7 Tage gespeichert und ausschließlich für Zwecke der Datensicherheit verwendet werden. Anlassbezogen können die Daten mit Zustimmung der/des Datenschutzbeauftragten im Einzelfall bei Bedarf auch länger gespeichert werden. In Abstimmung mit der/dem Datenschutzbeauftragten ist eine strikte Regelung zur Zweckbindung, zu den Berechtigungen und zum Umgang mit diesen Daten in den einzelnen Häusern zu etablieren.

14. Widget

Grundsatz: Keine Verwendung von Widgets, die Daten der Nutzerinnen und Nutzer verarbeiten

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 z.B. von Apple, Google und Microsoft angeboten.

Wenn der Dienstleister personenbezogene Daten wie die IP-Adresse der Nutzerinnen und Nutzer verarbeitet, ist dies datenschutzrechtlich relevant und berührt auch die Informationsfreiheit der „getrackten" Nutzerinnen und Nutzer. Daher ist diese Frage, ob personenbezogene Daten verarbeitet werden, unbedingt vor dem Einsatz eines Widgets zu klären.

15. Aktuelles Beispiel: Nutzung von Facebook Social Plugins („Gefällt mir"-Buttons)

Facebook gestattet anderen Webseitenbetreibern auf den eigenen Seiten „Gefällt mir"-Buttons und andere Elemente des Facebook-Netzwerkes einzubauen, sogenannte Social Plugins. Facebook kann auch ohne Betätigung des „Gefällt mir"-Buttons Nutzer bereits mit dem Aufruf der Seite, die das Plugin enthält (und nicht erst mit dem Anklicken des Social Plugins), identifizieren: Der Browser stellt nämlich gleichzeitig auch eine Verbindung zu den Servern von Facebook her. Der Inhalt des Plugins (das unter anderem die IP-Adresse enthält) wird von Facebook direkt an den Browser der Nutzerin/des Nutzers übermittelt und von diesem in die Webseite eingebunden. Facebook erhält so nicht nur einen Social Graph, wem was gefällt, sondern auch Informationen über einen Teil der Seiten, die Facebook-Nutzer im Netz besucht haben. Je mehr Seiten (auch der Rundfunkanstalten) die Social Plugins nutzen, desto umfassender kann Facebook das Surfverhalten von Nutzerinnen und Nutzern erfassen.

Dies ist datenschutzrechtlich unzulässig, da letztlich die IP-Adresse einer Nutzerin/eines Nutzers ohne Vorwarnung, ohne Wissen und möglicherweise gegen seinen Willen von dem eigentlichen Betreiber der Seite auch an Facebook geliefert wird – und das nur, weil die Nutzerin/der Nutzer auf eine bestimmte Seite geht, auf der dieses Plugin eingebaut ist. Dies verstößt gegen die Datenschutzbestimmungen der Rundfunkanstalten.

Daher wird von einem Einbau der Social Plugins von Facebook und anderer Widgets, die personenbezogenen Daten verarbeiten, auf den Seiten der Rundfunkanstalten grundsätzlich abgeraten.

16. Ausnahmsweiser Einbau von Widgets oder Social Plugins

Möchte eine Redaktion trotz der datenschutzrechtlichen Problematik ausnahmsweise ein Widget, mit dem personenbezogene Daten verarbeitet werden, nutzen, sollte ein klarer redaktioneller Nutzen für die Rundfunkanstalt und die Nutzerinnen und Nutzer ersichtlich sein.

In diesem Fall müssen die Rundfunkanstalten außerdem als Webseitenbetreiber die Verwendung von Widgets in ihren Datenschutzhinweisen erläutern.

Außerdem muss den Nutzerinnen und Nutzern die Möglichkeit eröffnet werden, das entsprechende Angebot auch ohne Widgets zu nutzen.

Eine etwaige ungewollte Übermittlung von Daten ist durch ein vorgeschaltetes Element zu unterbinden, das sie/den Nutzer in verständlicher Form darüber informiert, dass sie/er beim Anklicken Daten vom jeweiligen Anbieter lädt, und ihm die Wahlmöglichkeit lässt, die Seite mit dem Widget aufzurufen (2-Klick-Lösung).

17. Technische Aspekte

Medienbrüche (= Wechsel von einer Plattform oder einem Prozess auf eine/-n andere/-n mit der Gefahr der Informationsverfälschung) sollten weitestgehend verhindert werden, um eine höhere Revisionssicherheit zu gewährleisten.

Bei allen Angeboten sollte die nachträgliche Löschung und/oder Anonymisierung durch die Nutzerin/den Nutzer von vorne herein bei der Konzeption mit eingeplant werden.

III. BESONDERHEITEN BEI ANGEBOTEN FÜR MINDERJÄHRIGE

1. Verfahren
An Minderjährige gerichtete Social-Media-Angebote sollen nur nach einer Vorabbewertung durch die/den zuständige/n Datenschutzbeauftragte/n produktiv genommen werden. Eine Vorabbewertung soll auch bei einer wesentlichen inhaltlichen oder gestalterischen (prozessualen) Veränderung/Neuausrichtung bestehender Angebote erfolgen.

2. Inhaltliche Ausgestaltung
An Minderjährige gerichtete Angebote sollen hinsichtlich des Datenschutzes und der Datensicherheit den höchsten Maßstäben entsprechen, die für an Erwachsene adressierte Angebote derselben Rundfunkanstalt gelten.

Im Übrigen soll hinsichtlich der Anforderungen zu Datenschutz und Datensicherheit differenziert werden zwischen Angeboten

\ für Kinder, bei denen es sich um „Interneteinsteiger" handelt (etwa bis zum Alter von 13 Jahren; Gruppe 1) und
\ für Minderjährige, die erwartbar bereits Interneterfahrung besitzen und dazu tendieren, auch andere Onlineangebote mit geringerem Schutzniveau (kommerzielle Communities, usw.) zu nutzen (etwa ab dem Alter von 14 Jahren; Gruppe 2).

Bei Angeboten für die Gruppe 1 sollte eine Verknüpfung mit Drittangeboten nicht stattfinden. Die Erläuterungen zum Datenschutz sollten sowohl kindgerecht, als auch erwachsenengerecht erfolgen. Das Ziel ist, Kinder an das Thema Datenschutz heranzuführen und Eltern zu informieren. In Angeboten für Gruppe 2 sollten Verknüpfungen mit Drittangeboten unter den in D. genannten Voraussetzungen möglich sein, mit der Zielsetzung, einen verantwortungsvollen und aufgeklärten Umgang auch mit solchen Onlineangeboten zu vermitteln.

3. Einwilligung
Sofern Minderjährige unter 14 Jahren bei einem von der ARD betriebenen sozialen Netzwerk Mitglied werden dürfen – das zulässige Alter sollte in den Nutzungsbedingungen geregelt sein –, muss grundsätzlich die schriftliche Einwilligung der Erziehungsberechtigten zur Speicherung und Nutzung personenbezogener Daten der/des Minderjährigen ergänzend eingeholt werden.

Geeignet ist – in erster Linie bei Minderjährigen ab 14 Jahren – auch ein Double Opt-in-Verfahren, bei dem die Rundfunkanstalt der Minderjährigen/dem Minderjährigen an die von ihm anzugebende E-Mail-Adresse seiner Eltern/Erziehungsberechtigten die Einwilligungserklärung noch einmal per E-Mail übersendet und sich den Empfang durch die Eltern/Erziehungsberechtigten durch das Anklicken eines in die E-Mail integrierten Aktivierungslinks bestätigen lässt.

Ein Absehen von dem Erfordernis der Einwilligung der Eltern ist nur im begründeten Ausnahmefall und nach Rücksprache mit der/dem Datenschutzbeauftragten möglich.

D. Social-Media-Plattformen Dritter

Im Rahmen des Programmauftrags der Rundfunkanstalten kommen auch Kooperationen mit bestehenden, auch kommerziellen Anbietern von Social Media in Betracht. Die Rundfunkanstalten wirken darauf hin, dass bei derartigen Kooperationen die vorstehend beschriebenen datenschutzrechtlichen Anforderungen berücksichtigt werden.

I. ANFORDERUNGEN AN ANBIETER VON SOCIAL MEDIA

Sollten die Nutzungsbedingungen des Drittplattformbetreibers nicht den Datenschutzstandards der Rundfunkanstalten entsprechen, so haben die Rundfunkanstalten bei Interesse an einer Kooperation darauf hinzuwirken, dass im Rahmen der Zusammenarbeit die Einhaltung der datenschutz- und datensicherheitsrechtlichen Vorgaben der Landesrundfunkanstalten auf dieser Drittplattform sichergestellt ist.

Es muss insbesondere ausgeschlossen sein, dass das Nutzungsverhalten bezogen auf Inhalte der Rundfunkanstalten auf Plattformen Dritter durch diese Plattformen personenbezogen ausgewertet wird, soweit Nutzerinnen und Nutzer dem nicht ausdrücklich zustimmen. Die Drittplattformen dürfen außerdem in keinem Fall Daten über die Nutzung und das Nutzungsverhalten ihrer Userinnen und User an Dritte weitergeben.

Um eine Möglichkeit zur Durchsetzung dieser Position, insbesondere auch gegenüber den marktstarken Anbietern, zu haben, empfiehlt es sich, seitens der ARD insgesamt Rahmenbedingungen für die Präsenz eigener Angebote auf fremden Plattformen mit den jeweiligen Plattformbetreibern zu vereinbaren. Die zuständigen Datenschutzbeauftragten sollten bei entsprechenden Verhandlungen einbezogen werden.

Bei der Bewertung, inwieweit sich Anbieter von Social Media datenschutzkonform verhalten bzw. in Vereinbarungen auf Datenschutzkonformität verpflichtet werden können, ist – abgesehen vom nationalen Rechtsrahmen – ein Blick auf die Befassung der sogenannter Artikel-29-EU-Datenschutzgruppe hilfreich (vergleiche http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_de.pdf, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2010_05_12_l etter_art29wp_signatories_safer_social_networking_principles_en.pdf).

Kernpunkte für die Datenschutzkonformität sind danach:
SNS (= Social Network Services) erkennen die Anwendbarkeit der EG-Datenschutzrichtlinie auf die Verarbeitung personenbezogener Daten durch SNS auch dann an, wenn diese ihren Hauptsitz außerhalb des Europäischen Wirtschaftsraums haben. Die Anbieter sozialer Netzwerkdienste gelten als für die Verarbeitung Verantwortliche im Sinne der EG-Datenschutzrichtlinie.

Die Nutzerinnen und Nutzer gelten in Bezug auf die Verarbeitung ihrer personenbezogenen Daten durch die SNS als betroffene Personen. Die Verarbeitung personenbezogener Daten durch die Nutzerinnen und Nutzer selbst fällt in den meisten Fällen unter die Ausnahmeklausel für Privathaushalte.

SNS sollten ihre Nutzerinnen und Nutzer über ihre Identität aufklären und umfassende und eindeutige Informationen über ihre Zielsetzungen sowie über die verschiedenen Möglichkeiten vorlegen, wie sie die personenbezogenen Daten verarbeiten wollen. Werbemaßnahmen müssen im Einklang mit den einschlägigen Bestimmungen der EG-Datenschutzrichtlinie und der EG-Datenschutzrichtlinie für elektronische Kommunikation stehen.

SNS sollten datenschutzfreundliche Standardeinstellungen anbieten. SNS sollten den Nutzerinnen und Nutzern ausreichende Informationen und geeignete Warnhinweise zu den Risiken für den Schutz ihrer Privatsphäre an die Hand geben, die mit dem Hochladen von personenbezogenen Daten ins soziale Netzwerkprofil verbunden sind. SNS müssen sich festlegen, wie lange die Vorratsspeicherung von Daten inaktiver Nutzer im Höchstfall zulässig ist. Aufgegebene Nutzerprofile sind zu löschen.
SNS sollten besonders auf den Schutz Minderjähriger achten.
Den Nutzern sollte es im Allgemeinen gestattet sein, ein Pseudonym anzunehmen.

Die Nutzerinnen und Nutzer sollten vom SNS darauf hingewiesen werden, dass Bilder oder Informationen über dritte Personen nur mit der Einwilligung der betroffenen Person ins soziale Netzwerkprofil eingestellt werden sollten.

Die Homepage des SNS sollte zumindest einen Link zu einer Beschwerdestelle aufweisen, die sich mit den Datenschutzfragen der Mitglieder wie auch der Nichtmitglieder befasst.

II. NUTZUNG VON DRITTPLATTFORMEN, DIE NICHT DEN DATENSCHUTZRECHTLICHEN STANDARDS DER RUNDFUNKANSTALTEN ENTSPRECHEN

Sofern es nicht möglich ist, die datenschutzrechtlichen Standards für die Präsenz von Angeboten der Rundfunkanstalten auf Drittplattformen und deren Besuch durch Dritte mit den jeweiligen Plattformbetreibern zu vereinbaren, gilt Folgen des:

Es ist **vor** Nutzung der Drittplattform **ausdrücklich** und in jedem Einzelfall zu prüfen, ob der redaktionelle Mehrwert oder der Marketingmehrwert gegenüber bekannten Datenschutzmängeln, die insbesondere die Nutzer dieser Angebote treffen können, tatsächlich überwiegt.

Die meisten der größeren Anbieter von Social Media genügen leider momentan weder dem deutschen und dem europäischen Datenschutzrecht noch den Standards der ARD-Datenschutzbestimmungen. Einzelne Datenschutzbeauftragte vertreten die Auffassung, dass Unternehmen, die diese Plattformen zum Beispiel für Fanpages nutzen, auch für Datenschutzverstöße der Betreiber der Plattformen verantwortlich sind und gegebenenfalls auf Unterlassung der Nutzung in Anspruch genommen werden könnten. Dieser Position folgt der AK DSB in dieser Allgemeinheit nicht. Nicht genutzt werden sollten aber solche Dienste der Plattformbetreiber, bei denen Nutzerdaten ohne ausdrückliche Zustimmung ins außereuropäische Ausland übertragen werden. Dies trifft insbesondere auf Dienste zur Reichweitenmessung, wie beispielsweise „Insight“ von Facebook, zu.

Wegen der bekannten Einschränkungen bei der Einhaltung der deutschen Datenschutzgesetze und der ARD/ZDF/DLR-Standards sollte bei einem Link zu Facebook, Twitter, Google oder Ähnlichem immer ein deutlicher Hinweis zum Datenschutz platziert werden. Mit diesen Hinweisen ist die Nutzerin/der Nutzer dann ausreichend informiert und kann selbst entscheiden, ob er den Link auf die Drittplattform betätigt, sich dort erstmals registriert oder einloggt, um das Social-Media-Angebot der Rundfunkanstalt auf dieser Drittplattform zu nutzen.

Hier sind verschiedene Varianten denkbar: Bei allen Varianten sollte jedoch darauf hingewiesen werden, dass die Nutzungsbedingungen des Anbieters nicht den Datenschutzstandards der Rundfunkanstalt entsprechen. Zudem sollten dem Nutzer Hinweise gegeben werden, wie er seine Privatsphäre und seine persönlichen Daten auch bei Facebook, Twitter, Google und Anderen schützen kann.

Variante 1: Verlinkung auf Zwischenseite:
Bei Anklicken des Facebook-Links kommt man zunächst auf eine Zwischenseite, die den Datenschutzhinweis enthält:

Variante 2: Hinweis zu Datenschutz/Datensicherheit unmittelbar neben dem „Facebook"-Kasten

Variante 3: Popup mit Hinweise zum Datenschutz bei Anklicken des Facebook-Links

E. Maßnahmen zur Daten-/ Informationssicherheit

Damit der Datenschutz als rechtliches Ziel erreicht werden kann, sind technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten insbesondere vor Missbrauch, aber auch vor Verlust und Verfälschung erforderlich. Diese Maßnahmen müssen unter Berücksichtigung der gesetzlichen Regelungen, des Standes der Technik und der Kosten ein Schutzniveau gewährleisten, das mit Blick auf die von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden Daten angemessen ist.

In der Regel unterscheiden sich die Maßnahmen je nach Ausgestaltung des Angebots und nach den Besonderheiten in der Rundfunkanstalt.

I. ANGEBOTE AUF „EIGENEN" WEBSERVERN

\ Regelungen zu Datenschutz und IT-Sicherheit in der eigenen Rundfunkanstalt
\ Umsetzung technischer und organisatorischer Maßnahmen

II. ANGEBOTE AUF WEBSERVERN FEDERFÜHRENDER LANDESRUNDFUNKANSTALTEN

\ In der ARD abgestimmte Regelungen in Form von Vereinbarungen, zum Beispiel Anforderungen an Webanwendungen und Webserver im ARD CN

III. ANGEBOTE AUF WEBSERVERN VON DRITTEN, MIT DENEN VERTRÄGE ABGESCHLOSSEN WERDEN

\ Regelungen als Vertragsbestandteil
\ Einholung einer Bestätigung der Umsetzung von Sicherheitsmaßnahmen durch Abforderung Ausfüllung von Checklisten

IV. ANGEBOTE AUF WEBSERVERN VON DRITTEN OHNE EINFLUSS AUF DIE SICHERHEIT DER DATEN

\ Erstellung und Abstimmung von Entscheidungskriterien für die Nutzung von Social Media ohne vertraglichen Einfluss in den einzelnen Häusern
\ Risiken müssen bewertet und Verfahren zur Behandlung von Sicherheitsvorfällen wie zum Beispiel Datenschutzverletzungen und Verfälschung von Informationen etabliert werden.

Regelmäßig sind die Maßnahmen zur Informationssicherheit gemeinsam mit den für IT-Sicherheit Verantwortlichen zu erarbeiten. Ausführliche Hinweise sind beispielsweise in den folgenden Dokumenten enthalten.

\ Sicheres Bereitstellen von Webangeboten (vergleiche https://www.bsi.bund.de/ContentBSI/Themen/Internet_Sicherheit/WWW/ Webserver/isi-web-server.html)
\ Baustein B 5.4 „Webserver" BSI-IT-Grundschutz-Katalog (vgl.https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b 05/b05004.html)
\ Anforderungen an Webanwendungen und Webserver im ARD CN

Beispielhaft sei insbesondere auf folgende Datensicherheitsaspekte hingewiesen:

Sicherheit von Datenübertragung und Authentifizierungsmechanismen
Generell wird ein Webserver von außen über die HTTP-Schnittstelle angesprochen. Es ist auf eine ausreichende Sicherheit bei der Übertragung personenbezogener Daten und bei der Authentifizierung zu achten. So sollte beispielsweise beim Übertragungsvorgang sichergestellt sein, dass die übermittelten Daten im Kommunikationskanal zwischen dem Webbrowser der Nutzerin/des Nutzers und der Webanwendung des Dienstbetreibers verschlüsselt werden. Die Verschlüsselung HTTPS muss sich auf alle Daten inklusive der Log-in-Daten beziehen.

Sicherheit der Inhalte und Anwendungen auf dem Webserver
Um die Inhalte und Anwendungen auf dem Server vor unbefugtem Zugriff oder Veränderung zu schützen, ist es wichtig, die Rechte der verschiedenen beteiligten Benutzerinnen und Benutzer klar festzulegen. Die organisatorische und technische Realisierung der Trennung zwischen verschiedenen Benutzern, die eventuell Inhalte auf dem Server einstellen beziehungsweise pflegen dürfen, oder gar zwischen verschiedenen Webangeboten, die gemeinsam auf einem Server beheimatet sind, ist ein wichtiger Aspekt der Sicherheit eines Webangebots.

Technische Sicherheit des Webservers und der Webanwendung
Die Kompromittierung (= Angriff oder Schädigung) eines Webservers oder einer Webanwendung kann erhebliche finanzielle Verluste oder Imageschäden nach sich ziehen. Daher sind Webserver und Webanwendungen vor Angriffen aus dem Netz (also zum Beispiel über das Internet, aber auch aus dem Intranet heraus) zu schützen. Dabei müssen auch Schwachstellen des verwendeten Betriebssystems oder anderer verwendeter Softwareprodukte berücksichtigt werden.

Berücksichtigung von Datenschutz und IT-Sicherheitsaspekten bei Verträgen mit externen Dienstleistern, die auch mit personenbezogenen Daten der Nutzerinnen und Nutzer arbeiten
Sind externe Dienstleister mit Leistungen für das Onlineangebot der Rundfunkanstalt beauftragt, bei denen sie personenbezogenen Daten der Nutzerinnen und Nutzer verarbeiten, handelt es sich nach Datenschutzrecht regelmäßig um eine sogenannte Auftragsdatenverarbeitung, bei der einige formale und inhaltliche Anforderungen nach dem geltenden Datenschutzgesetz einzuhalten sind. Die Rundfunkanstalt bleibt trotz Einschaltung eines Dienstleisters für die persönlichen Daten ihrer Nutzerinnen und Nutzer datenschutzrechtlich verantwortlich. Die Vergabe des Auftrags hat daher unter besonderer Berücksichtigung der technischen und organisatorischen Eignung des Auftragnehmers zu erfolgen. Der Auftrag hat schriftlich zu erfolgen, wobei die Datenverarbeitung selber sowie die zugehörigen technischen und organisatorischen Maßnahmen zu beschreiben und die Anforderungen genau festzulegen sind. Zu diesen Maßnahmen gehört insbesondere auch die Gewährleistung der Auftragskontrolle. Die Auftragnehmer müssen den datenschutzrechtlich zuständigen Stellen ein entsprechendes Kontrollrecht einräumen. Der Auftragnehmer bleibt bezogen auf die Datenverarbeitung weisungsgebunden.

Ausführliche Hinweise hierzu sind beispielsweise in folgenden Dokumenten enthalten:
\ ISO 27001 Punkt
10.2 Management der Dienstleistungserbringung von Dritten
\ ISO 27002 Punkt
10.2.1 Erbringung von Dienstleistungen
10.2.2 Überwachung und Überprüfung der Dienstleistungen von Dritten
10.2.3 Management von Änderungen an Dienstleistungen von Dritten

F. Nutzung sogenannter Apps

Die Rundfunkanstalten veröffentlichen in Ergänzung zu bestimmten Sendungen bestimmte Teile ihres Angebots auch über sog. enannte Apps (z. B. Tagesschau, Sportschau, SWR3 Elchradio, MDR Sputnik2 und BR Rundschau), die auf mobilen wie stationären Endgeräten wie Smartphones, Tablets und Fernsehern und deren Betriebssystemen aufgerufen werden können.

Hauptnutzerinnen und -nutzer von Apps sind die Besitzerinnen und Besitzer eines Apple iPhone. Dafür werden die Apps vom iTunes App Store heruntergeladen. Voraussetzung zur Nutzung des App Stores ist ein Apple-Endgerät und eine Apple-ID mit folgenden Daten:

Name, Adresse, Telefonnummer, E-Mail-Adresse sowie Zahlungsdaten (Prepaid/Kreditkarte).

Apple nutzt die Daten der Apple-ID laut seiner Datenschutzrichtlinie über die Vertragsabwicklung hinaus für zahlreiche weitere Zwecke wie Produktentwicklung Analyse und Forschung.

Sofern ein User die „Genius"-Funktion nutzt, gewährt er dem Anbieter anonymisiert Einblicke in die Nutzungsgewohnheiten, wie zum Beispiel Anzahl der Starts der Produkte und Verwendungsdauer. Der mögliche Nutzen für Apple liegt in einem Kunden-/Konkurrenz- und Produktvergleich.

Zudem erlaubt Apples Datenschutzrichtlinie, personenbezogene Informationen anonymisiert an fremde – auch außerhalb der EU ansässige – Dienstleister weiterzugeben, die Kundenforschung und Produktentwicklung betreiben. Nach jüngst bekannt gewordenen Datenskandalen kann nicht ausgeschlossen werden, dass die von Apples beziehungsweise anderen Anbietern in ihren Datenschutzrichtlinien bzw. Nutzerhinweisen angekündigten Datenverwendungen nicht abschließend sind. Darauf sollten die Rundfunkanstalten in geeigneter Form hinweisen, sie sollten zugleich aber darauf hinweisen, dass diese Datenverarbeitung nicht in ihrer Verantwortung liegt.

Etwas anderes gilt für die Nutzerdaten in einer App, die von dem App-Entwickler/-Anbieter, also der Rundfunkanstalt, verarbeitet werden. Hier gilt Folgendes:

Es sollten ausführliche Datenschutzhinweise, die nicht versteckt sind und eine Kontaktmöglichkeit beinhalten, bereitgestellt werden.

Außer Zählpixeln und etablierter Webseitenprotokollierung sollte keine Protokollierung von Nutzerdaten stattfinden.

Die Apps sollten auch in alternativen App-Stores bereitgestellt werden. Es sollte Möglichkeiten zum direkten Download geben.

Es sollten Web-Apps statt nativer Apps verwendet werden.

Im Hinblick auf Datensparsamkeit und Datensicherheit sollten die Protokolldaten maximal 7 Tage gespeichert werden. Anlassbezogen können die Daten mit Zustimmung der/des Datenschutzbeauftragten im Einzelfall bei Bedarf auch länger gespeichert werden.

3. Stellungnahme zu den datenschutzrechtlich relevanten Bestimmungen des Entwurfs des 15. RfäSTV

(Stand 15. September 2010)

I. Summary

Wie auf der Besprechung in Hannover am 7. September 2010 bereits vorgetragen, hält der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) die datenschutzrechtlich relevanten Regelungen des Entwurfs des Rundfunkbeitragsstaatsvertrags bis auf einige wenige Ausnahmen für zulässig.

\ Die in § 2 Abs. 4 vorgesehene Unterscheidung zwischen verschiedenen Wohnungstypen und die Privilegierung von Nebenwohnungen sollte gänzlich entfallen, weil dann die auch intensiv in die Wohnung eingreifenden Ausforschungen überflüssig werden.

\ Die praktische Umsetzung von § 4 Abs. 1 Nr. 3 und § 4 Abs. 6 Satz 2 erscheint fraglich, weil nach den bisherigen Erfahrungen mit den Drittbescheiden nicht davon ausgegangen werden kann, dass die Sozialleistungsträger die benötigten Bescheinigungen ausstellen werden.

\ In § 4 Abs. 7 Satz 2 sollte auf die Erforderlichkeit einer Vorlage entsprechender Bescheide im Original oder in beglaubigter Kopie verzichtet und es sollten die Sozialleistungsträger gesetzlich verpflichtet werden, aussagekräftige Drittbescheinigungen über die Gewährung von Sozialleistungen auszustellen.

\ In § 4 Abs. 7 Satz 3 wäre eine Klarstellung zur Rechtsfolge im Falle der Beitragsermäßigung für die übrigen volljährigen Mitbewohnerinnen und Mitbewohner wünschenswert.

\ In § 4 Abs. 7 Satz 4 sollte der Verweis auf § 11 Abs. 5 aus redaktionellen Gründen gestrichen werden.

\ In § 8 Abs. 3 sollte eine umfassende und klarere Formulierung gewählt werden.

\ Zu § 8 Abs. 4 erscheint eine Klarstellung hinsichtlich des im Einzelfall zu erhebenden Datenkatalogs erforderlich. § 8 Abs. 4 Ziff. 4 sollte um Angaben zur konkreten Lage der Wohnung ergänzt werden.

\ In § 9 Abs. 1 Satz 4 ist die Notwendigkeit der Nennung weiterer Daten nicht ersichtlich. Falls es tatsächlich Konstellationen gibt, in denen die Kenntnis weiterer Daten erforderlich ist, sollte die Vorschrift zumindest konkretisiert werden.

\ In § 10 Abs. 7 Satz 2 sollte durch eine entsprechende Formulierung noch deutlicher als bislang klargestellt werden, dass keine Funktionsübertragung beabsichtigt ist.

\ Da sich § 11 Abs. 2 Satz 1 lediglich auf die in § 10 Abs. 7 erwähnte, im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle bezieht, sollte in § 11 Abs. 2 Satz 1 durch eine entsprechende Formulierung klargestellt werden, dass hier die in § 10 Abs. 7 genannte Stelle gemeint ist.

\ In § 11 Abs. 2 Satz 3 sollte auf das Datenschutzrecht des Sitzlandes verwiesen werden.

\ In § 11 Abs. 4 Satz 1 müssen die Zwecke „Beitragsbefreiung“ und „Beitragsermäßigung“ gestrichen werden. Durch die Ergänzung des Grundsatzes der Direkterhebung am Ende des Satzes 1 sollte deutlich werden, dass die Datenerhebung bei Dritten ohne Kenntnis der Betroffenen/des Betroffenen Ultima Ratio ist.

\ In die Aufzählung in § 11 Abs. 5 Satz 1 sollten auch die nach Abs. 4 erhobenen Daten aufgenommen werden. In § 14 Abs. 9 Ziff. 7 sollte nur die letzte Anschrift (Singular) von Haupt- und Nebenwohnungen genannt werden.

\ Die 2-Jahres-Frist beim einmaligen Abgleich mit Einwohnermeldedaten gemäß § 14 Abs. 9 ist ausdrücklich als Höchstfrist zu kennzeichnen. Es wird angeregt, zumindest eine entsprechende Klarstellung in die Gesetzesbegründung aufzunehmen.

II. Im Einzelnen

ZU § 2 ABS. 4

Eines der zentralen Anliegen des neuen Modells ist es, die Datenerhebungen im privaten Bereich zu reduzieren, weil nur noch an die Wohnung als solche angeknüpft wird und nicht mehr die Verhältnisse in der Wohnung erforscht werden müssen (“keine Prüfung hinter der Wohnungstür”). Mit der Einteilung von Wohnungen in unterschiedliche Kategorien und der Privilegierung von Nebenwohnungen (soweit nicht Hauptwohnung eines Dritten) wird aber wieder eine Datenerhebung durch Ausforschung bei den Privatwohnungen zum Beispiel durch Beauftragte nötig. Es müssen zunächst die einzelnen Wohnungsbewohnerinnen und -bewohner festgestellt werden und dann muss geprüft werden, für wen die Wohnung jeweils eine Haupt- oder Nebenwohnung ist. Der Grundsatz der Datenminimierung wird damit verlassen. Es sollte deshalb die Unterscheidung zwischen verschiedenen Wohnungstypen und die Privilegierung von Nebenwohnungen gänzlich entfallen, weil dann auch intensiv in die Wohnung eingreifende Ausforschungen überflüssig werden.

Ergebnis: § 2 Abs. 4 wird ersatzlos gestrichen. Der bisherige § 2 Abs. 5 wird Abs. 4.

ZU § 4 ABS. 1 NR. 3

Hier findet sich eine Neuregelung dergestalt, dass eine Befreiung künftig gewährt wird, wenn der Zuschlag nach § 24 SGB II die Höhe des Rundfunkbeitrags nicht übersteigt. Gegen diese Regelung als solche ist aus datenschutzrechtlicher Sicht nichts einzuwenden, allerdings dürfte die Umsetzung ähnlich problematisch wie die Umsetzung der Härtefallregelung in Abs. 6 sein, weil die Höhe des Zuschlags bisher nur den Leistungsbescheiden, nicht aber den Drittbescheinigungen zu entnehmen ist. Es müsste gelingen, die Argen und andere Sozialleistungsträger dazu zu bewegen, die Tatsache, dass der Zuschlag gemäß § 24 SGB II die Höhe des Rundfunkbeitrags nicht überschreitet, in die Drittbescheinigungen aufzunehmen. Ansonsten müssten die Rundfunkanstalten – entgegen des Grundsatzes der Datensparsamkeit – wieder den Leistungsbescheid beziehungsweise Teile davon einfordern, um das Vorliegen der Befreiungsvoraussetzungen zu überprüfen. Außerdem gibt es offenbar Fälle, in denen für bestimmte Zeiträume eines einheitlichen Leistungsbescheids unterschiedlich hohe Zuschläge gezahlt werden. Ob die Argen überhaupt technisch in der Lage sein werden, dies in den Drittbescheiden aufzuführen, ist nicht bekannt. Eine datenschutzkonforme praktische Umsetzung dieser Regelung ist daher fragwürdig.

ZU § 4 ABS. 6 SATZ 2

Die Regelung erscheint zu unbestimmt. Unklar ist beispielsweise die Dauer des Befreiungszeitraums.

Zudem stellt sich auch hier die Frage nach der praktischen Umsetzung der Regelung. Problematisch ist, ob und auf welche Weise mit einem Bescheid nachgewiesen werden kann, dass die Versagung einer der Sozialleistungen nach Abs. 1 Nr. 1 bis 9 darauf beruht, dass die maßgeblichen Einkünfte die jeweilige Bedarfsgrenze um weniger als die Höhe des Rundfunkbeitrages überschreiten.

Es erscheint fraglich, ob die Argen et cetera gesonderte Ablehnungsbescheide ausstellen, die sich auf bestimmte Daten beschränken und dann bei den Landesrundfunkanstalten beziehungsweise der GEZ eingereicht werden können. In der Praxis wird bereits heute in vielen Fällen z.B. bei der Gewährung von BaföG seitens der Behörden offen gelassen, ob ein Anspruch besteht oder nicht, weil jedenfalls dann, wenn ein Anspruch bestehen würde, nur ein Betrag erreicht würde, der nicht zur Auszahlung gelangt. Diese Entscheidung erfolgt nicht in Bescheidform. Weder die Rundfunkanstalten noch die nachfolgend angerufenen Gerichte können in solchen Fällen ohne Vorlage entsprechender Bescheinigungen eigene Berechnungen anstellen. Auch bei den eine Leistung zusprechenden Bescheiden sind nach den Erfahrungen der GEZ noch lange nicht alle Stellen flächendeckend bereit oder dazu in der Lage, die geforderten Drittbescheinigungen auszustellen.

ZU § 4 ABS. 7 SATZ 2

Aus datenschutzrechtlicher Sicht wird gefordert, die Erforderlichkeit für eine Vorlage entsprechender Bescheide im Original oder in beglaubigter Kopie zu beseitigen. Derartige Bescheide enthalten nämlich in vielen Fällen sensible Daten, die für die Gewährung der Befreiung nicht benötigt werden. Voraussetzung ist, dass die Sozialleistungsträger gesetzlich verpflichtet werden, aussagekräftige Drittbescheinigungen über die Gewährung von Sozialleistungen auszustellen.

Ergebnis: § 4 Abs 7 Satz 2 ist entsprechend zu ändern.

ZU § 4 ABS. 7 SATZ 3

In § 4 Abs. 3 ist geregelt, dass sich die der Antragstellerin/dem Antragsteller gewährte Befreiung oder Ermäßigung innerhalb der Wohnung nur auf bestimmte Personengruppen (zum Beispiel Ehegatten und eingetragene Lebenspartnerinnen und Lebenspartner) erstreckt. Daraus kann im Fall der Befreiung geschlossen werden, dass von den nach dieser Vorschrift nicht privilegierten Mitbewohnerinnen und Mitbewohnern der befreiten Person eine Person den Beitrag leisten muss. Das Teilnehmerkonto ist auf diejenige Person umzuschreiben, für die kein Befreiungsgrund und daher eine Anmelde- und Zahlungspflicht besteht. Offen ist, was im Falle der Ermäßigung gilt. Aus datenschutzrechtlicher Sicht wäre eine klare gesetzliche Regelung zu begrüßen, aus der hervorgeht, dass anstelle der Beitragsschuldnerin/des Beitragsschuldners mit ermäßigtem Beitrag eine Mitbewoherin/ein Mitbewohner ohne Befreiungs- bzw. Ermäßigungsgrund den vollen Beitrag zu leisten hat.

ZU § 4 ABS. 7 SATZ 4

Die Regelung in Satz 4, wonach § 11 Abs. 5 entsprechend gilt, widerspricht dem Wortlaut von § 11 Abs. 5 Satz 1. Danach soll § 11 Abs. 5 im Falle des § 4 Abs. 7 nicht entsprechend, sondern unmittelbar zur Anwendung kommen (siehe dazu Wortlaut des § 11 Abs. 5).

Ergebnis: § 4 Abs. 7 Satz 4 sollte ersatzlos gestrichen werden.

ZU § 8 ABS. 3

Die Formulierung im zweiten Halbsatz („ …sofern sich für die Wohnung, Betriebsstätte oder das Kraftfahrzeug keine Änderung der Beitragspflicht ergibt… “) ist missverständlich. Es müsste deutlich gemacht werden, wer als Teilnehmerin/Teilnehmer zu melden ist, wenn in einer Wohnung sowohl Personen leben, die Befreiungs- oder Ermäßigungsgründe geltend machen können, als auch Personen, für die dies nicht gilt. Erforderlich ist hier eine gesetzliche Klarstellung, aus der sich ergibt, wer anzeige- und beitragspflichtig ist und wessen Daten daher zu speichern sind.

Ergebnis: § 8 Abs. 3 sollte wie folgt ergänzt werden:

„Besteht für einzelne Inhaberinnen und Inhaber einer Wohnung die Möglichkeit, eine Befreiung oder Ermäßigung im Sinne des § 4 zu beanspruchen, so ist von mehreren Wohnungsinhaberinnen und -inhabern (Beitragsschuldnerinnen und -schuldnern) im Zweifel derjenige anzeige- und beitragspflichtig, der keine Voraussetzungen einer Befreiung oder Ermäßigung gemäß § 4 Abs. 7 Satz 2 nachweisen kann. Liegen bei allen Inhaberinnen und Inhabern einer Wohnung Gründe im Sinne des § 4 Abs. 7 Satz 2 vor, so ist im Zweifel derjenige anzeige- und beitragspflichtig, der lediglich eine Ermäßigung gemäß § 4 Abs. 2 geltend machen kann. Die Vorschrift des § 4 Abs. 3 bleibt unberührt."

ZU § 8 ABS. 4

Mit dieser Vorschrift sollen insgesamt mindestens vier Sachverhalte geregelt werden: 1. die echte Neuanmeldung, 2. die Ummeldung, 3. die Anmeldung, nachdem die bisherige Zahlerin/der bisherige Zahler aus der Wohnung ausgezogen ist und 4. die Änderungsmeldung gemäß § 8 Abs. 1 Satz 1 Hs.

Es wird nicht zwischen dem privaten und nichtprivaten Bereich unterschieden. Je nach Sachverhalt ist aber die Erhebung unterschiedlicher Daten erforderlich. Allerdings liegt es auf der Hand, dass gemäß dem datenschutzrechtlichen Grundsatz der Erforderlichkeit jeweils nur diejenigen Daten angegeben werden müssen, die im Einzelfall erforderlich sind. In gleicher Weise ist die entsprechende Regelung in § 3 Abs. 2 RGebStV ausgelegt und angewendet worden. Dennoch erscheint eine entsprechende Klarstellung in der Gesetzesbegründung sinnvoll.

Ziffer 4 sollte um die Angaben ergänzt werden, die der Identifizierung der konkreten Wohnung dienen können (Lage der Wohnung, Etage, Wohnungsnummer). Die Übermittlung dieser Angaben würde gegebenenfalls weitere Ermittlungen vor Ort überflüssig machen.

Ergebnis: § 8 Abs. 4 Ziff. 4 sollte wie folgt ergänzt werden:

„gegenwärtige Anschrift einschließlich konkreter Lage jeder Wohnung und jeder Betriebsstätte"

ZU § 9 ABS. 1

Satz 1
Das Auskunftsrecht in Satz 1 entspricht § 4 Abs. 5 Satz 1 RGebStV und ist ein notwendiges Instrument zur Klärung der Beitragspflicht. Tatsächliche Anhaltspunkte können beispielsweise das Namensschild auf dem Klingelschild sein.

Satz 2
Das Auskunftsrecht gegenüber der Eigentümerin/dem Eigentümer und den vergleichbar dinglichen Berechtigten ist unter den Voraussetzungen nach § 9 Abs. 1 Satz 2 datenschutzrechtlich zulässig.

Zwar wird damit von dem Grundsatz der Direkterhebung personenbezogener Daten abgewichen, eine Überprüfung im Hinblick auf den Grundsatz der Verhältnismäßigkeit ergibt aber, dass dieses Auskunftsrecht als Ultima Ratio ein geeignetes Mittel ist, um eine Beitragsschuldnerin/einen Beitragsschuldner zu ermitteln. Eine Abwägung hat zwischen dem Persönlichkeitsrecht des Einzelnen (der Preisgabe ihres/seines Namens/seiner Daten durch einen Dritten ohne ihr/sein Wissen) und dem öffentlichen Interesse an der vollständigen Erfassung aller Beitragsschuldnerinnen und -schuldner im Interesse der Beitragsgerechtigkeit zu erfolgen. In dem Fall, in dem die Inhaberin/der Inhaber einer Wohnung oder Betriebsstätte (= gesetzliche Beitragsschuldnerin/ gesetzlicher Beitragsschuldner) nicht anders auffindbar ist, erscheint es gerechtfertigt, dass deren/dessen Recht auf informationelle Selbstbestimmung (beziehungsweise. auf Anonymität) eingeschränkt wird.

Aus der Tatsache, dass die Geltendmachung des Auskunftsanspruchs gegenüber dem Eigentümer Ultima Ratio ist („Kann die zuständige Landesrundfunkanstalt den Inhaber einer Wohnung oder Betriebsstätte nicht feststellen…"), folgt, dass zunächst versucht werden muss, die erforderlichen Daten direkt bei demjenigen zu erheben, bei dem tatsächliche Anhaltspunkte vorliegen (Satz 1).

Die Eigentümerin/Der Eigentümer ist die/der dinglich am stärksten Berechtigte, die/der den Besitz an die Inhaberin/den Inhaber vermittelt, und der deshalb am besten darüber Auskunft geben kann, wer nun der Inhaber ist. Zudem rückt sie/er allein aufgrund seines Eigentums am Grundstück zur Recht in den Fokus als potenzielle Wohnungsbewohnerin/potentieller Wohnungsbewohner bzw. Firmenin-haber. Die Eigentümerin/Der Eigentümer lässt sich notfalls leicht über das öffentlich zugängliche Grundbuch ermitteln. Die Belastung für die Eigentümerin/den Eigentümer ist letztlich auch sehr gering, da er für eine leer stehende Wohnung beziehungsweise Betriebsstätte gar nicht als Beitragsschuldnerin/Beitragsschuldner herangezogen wird und ansonsten nur auf die derzeitige Inhaberin/den derzeitigen Inhaber verweisen muss, um den Auskunftsanspruch und ein mögliches Verwaltungszwangsverfahren/Zwangsgeld abzuwehren.

Satz 4
Die Regelung in § 9 Abs. 1 Satz 4 entspricht dem bisherigen § 4 Abs. 5 Satz 3 RGebStV. Auch wenn es an dieser Regelung bislang keine Kritik gab, ist festzustellen, dass diese Regelung sehr weit gefasst ist. Unklar ist, welche weiteren Daten hier überhaupt gemeint sein können. Mit dem Wegfall der Mehrfachgebührenpflicht fallen möglicherweise auch die bislang erforderlichen weiteren Daten weg (zum Beispiel die Angabe, ob eine Minderjährige/ein Minderjähriger im gemeinsamen Haushalt bereits selbst über ein eigenes Einkommen verfügt, et cetera). Es sollte daher noch einmal geprüft werden, ob diese Regelung tatsächlich noch benötigt wird. Eventuell trifft der Bedarf auch nur für den Bereich der Betriebsstätten zu. Dann sollte dies in der Formulierung zum Ausdruck kommen.
Der Verweis im 2. Hs. auf § 11 Abs. 5 entfällt.

Satz 5
In Satz 5 müsste bei Streichung des Satzes 4 auch die Passage: „und die Daten nach Satz 4“ entfallen.

ZU § 10 ABS. 7 SATZ 2

Durch die Formulierung in Satz 2 ist eine Funktionsübertragung nicht eindeutig ausgeschlossen. Es wird daher vorgeschlagen, das Wort „ermächtigt“ durch „dürfen“ zu ersetzen, da für die hier angesprochene Auftragsdatenverarbeitung keine Ermächtigung erforderlich ist. Außerdem sollten die Worte „ganz oder teilweise“ gestrichen werden.

Ergebnis: § 10 Abs. 7 Satz 2 sollte wie folgt formuliert werden:

„Die Landesrundfunkanstalt darf einzelne Tätigkeiten bei der Durchführung des Beitragseinzugs und der Ermittlung von Beitragsschuldnern auf Dritte übertragen.“

ZU § 11 ABS. 2 SATZ 1

Da sich § 11 Abs. 2 Satz 1 lediglich auf die in § 10 Abs. 7 erwähnte, im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle bezieht, sollte in § 11 Abs. 2 Satz 1 durch eine entsprechende Formulierung klargestellt werden, dass hier die in § 10 Abs. 7 Satz 1 genannte Stelle gemeint ist.

Ergebnis: § 11 Abs. 2 Satz 1 sollte wie folgt formuliert werden:

„Bei der gemäß § 10 Abs. 7 Satz 1 im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebenen Stelle ist unbeschadet der Zuständigkeit der/des nach Landesrecht für die Landesrundfunkanstalt zuständigen Datenschutzbeauftragten eine behördliche Datenschutzbeauftrragte/ein behördlicher Datenschutzbeauftragter zu bestellen.“

ZU § 11 ABS. 2 SATZ 3

Soweit in Abs. 2 Satz 3 ein Hinweis auf das im Übrigen geltende BDSG erfolgt, sollte stattdessen auf die datenschutzrechtlichen Regelungen des Sitzlandes der Stelle nach § 10 Abs. 7 Satz 1 erfolgen.

Ergebnis: § 11 Abs. 2 Satz 3 sollte wie folgt formuliert werden:

„Im Übrigen gelten die für den behördlichen Datenschutzbeauftragten anwendbaren Bestimmungen des Sitzlandes der in § 10 Abs. 7 Satz 1 genannten Stelle.“

ZU § 11 ABS. 4

Satz 1
Diese Vorschrift muss konkretisiert werden. Die Berechtigung, für alle genannten Zwecke Daten ohne Kenntnis der Betroffenen bei Dritten zu erheben, geht zu weit. Die Zwecke „Beitragsbefreiung“ und „Beitragsermäßigung“ müssten gestrichen werden. Es besteht auch kein Bedürfnis für eine derartige Regelung. Bliebe es bei dieser weitreichenden Regelung, könnte daraus gegebenenfalls sogar eine Pflicht zur Amtsermittlung gefolgert werden (kein Unterlaufen des Antragsprinzips). Im Übrigen sind diese Fälle auch nicht mit den in Satz 2 genannten Voraussetzungen kompatibel.

Für die Fälle „Beitragserhebung“ und „Feststellung, ob eine Beitragspflicht nach diesem Staatsvertrag besteht“ sollte durch die Ergänzung des Grundsatzes der Direkterhebung am Ende des Satzes 1 entsprechend § 4 Abs. 6 Satz 1 Hs. 2 RGebStV deutlich werden, dass die Datenerhebung bei Dritten ohne Kenntnis der/des Betroffenen Ultima Ratio ist.

Die Datenerhebung bei nichtöffentlichen Stellen (Adressanmietung zum Zwecke von Mailingmaßnahmen) bleibt als Ultima Ratio auch weiterhin erforderlich. Weder durch den einmaligen Datenabgleich mit den Einwohnermeldeämtern noch durch die regelmäßige Einwohnermeldedatenübermittlung werden diejenigen Personen erfasst, die sich bei den Meldebehörden nicht an- bzw. nicht ummelden. Zudem bleibt die Adressanmietung künftig vor allem für den gesamten gewerblichen Bereich von Bedeutung. Dies ist auch vor dem Hintergrund zu sehen, dass der Beauftragtendienst vor Ort erheblich reduziert werden soll.

Sätze 3 und 4
Die Sätze 3 und 4 sollten ebenfalls gestrichen werden, weil derselbe Text in §11 Abs. 5 nochmals erscheint.

Ergebnis: § 11 Abs. 4 sollte wie folgt formuliert werden:

„Für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach diesem Staatsvertrag besteht, kann die zuständige Landesrundfunkanstalt personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis der/des Betroffenen erheben, verarbeiten oder nutzen, soweit die Erhebung der Daten bei der/beim Betroffenen nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Voraussetzung dafür ist, dass (...)“

die Datenbestände dazu geeignet sind, Rückschlüsse auf die Beitragspflicht zuzulassen, insbesondere durch Abgleich mit dem Bestand der bei den Landesrundfunkanstalten gemeldeten Beitragsschuldnerinnen und -schuldnern, und sich die Daten auf Angaben beschränken, die der Anzeigepflicht nach § 8 unterliegen, und kein erkennbarer Grund zu der Annahme besteht, dass die/der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat. Daten, die Rückschlüsse auf tatsächliche oder persönliche Verhältnisse liefern könnten, dürfen nicht an die übermittelnde Stelle rückübermittelt werden.“

ZU § 11 ABS. 5 SATZ 1:

In die Aufzählung sollten auch die nach Abs. 4 erhobenen Daten aufgenommen werden. Ergebnis: § 11 Abs. 5 sollte wie folgt formuliert werden:

„Die Landesrundfunkanstalt darf die in § 4 Abs. 7, § 8 Abs. 4 und 5 und § 9 Abs. 1 genannten Daten, sonstige freiwillig übermittelte Daten und die nach Abs. 4 erhobenen Daten nur für die Erfüllung der ihr nach diesem Staatsvertrag obliegenden Aufgaben erheben, verarbeiten und nutzen."

ZU § 14 ABS. 9

Die einmalige Übermittlung der in der Vorschrift im Einzelnen aufgeführten Daten aller volljährigen Personen an die jeweilige Landesrundfunkanstalt zum Zwecke der Bestands- und Ersterfassung ist verfassungsgemäß.

Die Maßnahme ist zur Erreichung des Zwecks der Bestands- und Ersterfassung geeignet. Nach Abgleich mit den bereits in der Rundfunkteilnehmerdatenbank vorhandenen Daten und sofortiger Löschung der Daten von Personen, bei denen man anhand bestimmter Kriterien wie zum Beispiel Namensgleichheit mit einer hohen Wahrscheinlichkeit davon ausgehen kann, dass sie mit einer bereits registrierten Person in einer Wohnung zusammenwohnen, werden die übrig bleibenden Personen von den Rundfunkanstalten zur Feststellung der Beitragspflicht angeschrieben.

Die Tatsache, dass jemand nach dem Melderecht für eine bestimmte Wohnung gemeldet ist, begründet die Vermutung, dass sie/er bezogen auf diese Wohnung Beitragsschuldnerin/Beitragsschuldner ist (vergleiche § 2 Abs. 2 Nr. 1). Falls die konkrete Wohnung nicht bekannt ist, dürfte die Tatsache, dass er überhaupt unter einer bestimmten Adresse gemeldet ist, als tatsächlicher Anhaltspunkt für die Beitragsschuldnerstellung im Sinne von § 9 Abs. 1 Satz 1 genügen. In beiden Fällen besteht also eine Verpflichtung zur Auskunft, die nach § 9 Abs. 1 letzter Satz im Verwaltungszwangsverfahren durchgesetzt werden kann.

Der Zweck der Bestands- und Ersterfassung lässt sich auch nicht durch mildere Mittel erreichen. Der regelmäßige Meldedatenabgleich ist nicht ebenso wirksam wie die einmalige Datenübermittlung sämtlicher volljähriger Personen, denn es gibt viele Menschen, die nur selten umziehen und daher mit den Mailings aufgrund regelmäßigen Meldedatenabgleichs nicht erreicht werden können. Die von privaten Adresshändlern bezogenen Adressdaten beinhalten nicht die über die reine Adresse hinaus ebenfalls wichtigen Daten wie Geburtsdatum, Tag des Einzugs, et cetera. Außerdem sind sie nicht vergleichbar verlässlich wie die EMA-Daten. Auch mit dem Instrument der Gruppenauskünfte könnte man nur einen Bruchteil der benötigen Daten erhalten. Das Gleiche gilt für die vom Beauftragtendienst zu erlangenden Daten, wobei zu beachten ist, dass die Arbeit des Beauftragtendienstes ohnehin kein milderes Mittel ist. Die Schwere des Eingriffs steht bei einer Gesamtabwägung auch nicht außer Verhältnis zu dem Gewicht, der ihn rechtfertigenden Gründe. Zwar ist das Recht auf informationelle Selbstbestimmung aller volljährigen Personen in Deutschland durch die Datenübermittlung von den Einwohnermeldebehörden an die Landesrundfunkanstalten bzw. die GEZ berührt, allerdings ist zu berücksichtigen, dass ein Großteil dieser Daten nach Abgleich mit der GEZ-Datenbank der Rundfunkgebührenzahlerinnen und -zahler sogleich wieder gelöscht wird. Diejenigen, die bereits Gebühren zahlen, werden nicht weiter behelligt. Diejenigen jedoch, die angeschrieben werden, weil sie bislang nicht zahlen, müssen es hinnehmen, von den Landesrundfunkanstalten zum Zwecke der Geltendmachung des Auskunftsanspruchs angeschrieben und zur Antwort verpflichtet zu werden. Denn es ist davon auszugehen, dass sämtliche Angeschriebenen als Inhaberin/Inhaber einer Wohnung nach dem Rundfunkbeitragsstaatsvertrag ohnehin für einen Rundfunkbeitrag gesamtschuldnerisch haften und nach dem Rundfunkbeitragsstaatsvertrag zur Auskunft verpflichtet sind.

Nachdem die Landesrundfunkanstalten bzw. die GEZ darlegen, dass sie bei Erhalt sämtlicher Daten zu einem einzigen Stichtag diese aus technischen und organisatorischen Gründen nicht innerhalb eines Jahres abgleichen, Mailings ausbringen und den Rücklauf bearbeiten könnten, ist die 2-Jahres-Frist ausdrücklich als Höchstfrist zu kennzeichnen. Eine entsprechende Klarstellung sollte jedenfalls zumindest in die Gesetzesbegründung aufgenommen werden.

ZU § 14 ABS. 9 ZIFFER 7

In § 14 Abs. 9 Ziffer 7 ist lediglich die letzte Anschrift von Haupt- und Nebenwohnungen einschließlich aller vorhandenen Angaben zur Lage der Wohnungen erforderlich, um eine eindeutige Zuordnung vornehmen können. Weitere vorhergehende Anschriften dürfen daher nicht abgefragt werden.

Ergebnis: § 14 Abs. 9 Ziffer 7 sollte wie folgt formuliert werden:

„gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen einschließlich aller vorhandenen Angaben zur Lage der Wohnung und"

Saarbrücken, 7. Oktober 2010

ANHANG: 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.

4. DATENVERARBEITUNG

Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten (§ 3 Abs. 4 Satz 1 BDSG).

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
Marketing
Appellhofplatz 1
50667 Köln

Redaktion
Beate Ritter
Datenschutzbeauftragte

Stand November 2013

WESTDEUTSCHER
RUNDFUNK

Appellhofplatz 1
50667 Köln

www.wdr.de