14. Tätigkeitsbericht

der Beauftragten für den Datenschutz
des
Rundfunk Berlin-Brandenburg

Berichtszeitraum:

01. April 2016 bis 31. März 2018

Dem Rundfunkrat gemäß § 38 Abs. 7 **rbb**-Staatsvertrag
vorgelegt von
Anke Naujock

Inhaltsverzeichnis

Inhaltsverzeichnis I

Vorbemerkung 1

A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg 3

I. Gesetzliche Grundlagen 3
II. Konkrete Situation 4

B. Entwicklung des Datenschutzrechts 5

I. Europa 5

1. Normen und Abkommen 5
1.1 EU-Datenschutz-Grundverordnung 5
1.2 ePrivacy-Verordnung 7
1.3 Privacy Shield 8

2. Gerichtliche Entscheidungen 9
2.1 EuGH-Urteil zur Speicherung dynamischer IP-Adressen durch Website-Betreiber 9
2.2 EuGH-Urteil zur Haftungsfreistellung von WLAN-Anbietern 10
2.3 EuGH-Urteil zur Vorratsdatenspeicherung 11

II. Bund 12

1. Normen 12
1.1. Bundesdatenschutzgesetz nF 12
1.2 Telemediengesetz 18
1.3 Netzwerkdurchsetzungsgesetz 18

2. Gerichtliche Entscheidungen 19
2.1 Urteile des Bundearbeitsgerichts zu verdeckten Maßnahmen gegenüber Arbeitnehmern 19
2.2 Urteil des OLG Frankfurt a. M. vom 05.10.2017 zur Aufklärungspflicht bei Vertrieb von Smart-TV 21

III. Berlin/Brandenburg 21

1. Normen 21
1.1 21. Rundfunkänderungsstaatsvertrag 21
1.2 Berliner Datenschutzgesetz nF 22
1.3 Verordnungen zur Durchführung des Meldegesetzes (DVO Meldegesetz) ... 23

1.4 Rundfunkbeitragssatzung 24

2. Gerichtliche Entscheidungen 25
2.1 Urteil des Oberverwaltungsgerichts Berlin-Brandenburg vom 29.11.2017 zurRechtmäßigkeit der Rundfunkbeitragssatzung 25
2.2 Zwei Beschlüsse des Verwaltungsgerichts Berlin zum presserechtlichen Auskunftsanspruch des rbb 26
2.3 Beschlussverfahren Freienvertretung ./. rbb 28

C. Datenschutz und Datensicherheit im rbb 29

I. Neue Regelwerke 29

1. Dienstanweisung zur Konfliktregulierung im rbb 29
2. Dienstvereinbarung über die Nutzung mobiler Telekommunikationsgeräte. 30
3. Rahmendienstvereinbarung über elektronische Zutrittskontrolleinrichtungen und Videoüberwachungsanlagen 31
4. Dienstanweisung IT-Nutzung 31

II. Projekte und Arbeitsgruppen 32

1. Projekt Umsetzung DSGVO 32
2. Jour Fixe IT-Projekte 33
3. Informationssicherheitskreis 34

III. Aktuelle IT-Projekte 35

1. Umstieg auf das neue Betriebssystem Windows 10 35
2. Probebetrieb "MS Office 365" in der Europa-Cloud 35
3. OpenMedia/Multimediales Redaktions- und Planungssystem (MPRS) 38
4. Video Produktions Management System VPMS 39
5. Unified Communication 40
6. HTTPS-Proxy 41
7. Notfall-App 42
8. Software-Lizenz-Management-System "Snow Software" 43
9. ASPR - Passwort Reset Manager 44
10. Neues Fuhrparkmanagementsystem 46
11. Neues Materialdispositionssystem "Easyjob" 46

IV. Beschäftigtendatenschutz 47

1. Umsetzung der SAP-Dienstvereinbarungen 47
2. Versand elektronischer Gehaltsabrechnungen 47
3. Elektronisches Firmenticket 48
4. Bewerbermanagementsystem Umantis 49
5. Einsatz von Videokameras zur Dokumentation von Baufortschritten 50
6. Gefährdungsbeurteilung psychischer Belastungen 51
7. Anonymes Hinweisgebersystem 51
8. Bring your own device 52

9. Übermittlung von Vergütungsdaten an die Kommission zur Ermitttlung des Finanzbedarfs ... 53
10. Zuverlässigkeitsüberprüfung im Zusammenhang mit Akkreditierungen ... 54
11. Veröffentlichungen von Statistiken zum Frauenförderplan ... 56
12. Datenschutzrechtliche Aspekte bei der Auslegung des Freienstatuts ... 57
13. #metoo ... 57
14. E-Learning ... 58

V. Datenschutz in den Angeboten des rbb ... 59

1. Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten ... 59
2. Datenschutzregelungen im Lizenzvertrag der Rundfunkanstalten mit der AGF GmbH ... 59
3. TVswift ... 60
4. RadioAnalyzer ... 61
5. Neues Medienangebot von ARD und ZDF für Jugendliche und junge Erwachsene "funk" ... 62
6. Verbreitung von Informationen von Inforadio per WhatsApp oder Telegram ... 63
7. Archivierung von Tweets und Kommentaren im rbb-Archiv ... 64
8. LU-Smart-App ... 64
9. Vereinbarkeit von Medienprivileg und Recherche-Zugriff für Verwertungstöchter und Auftragsproduzenten ... 65

VI. Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung ... 66

1. Allgemeines ... 66
2. Auskunftsersuchen und Eingaben ... 67
3. Projekt EUDAGO ... 69
4. Vorbereitungen für den weiteren Meldedatenabgleich ... 70
5. Überarbeitung Historielöschkonzept ... 71

D. Datenschutz im Informationsverarbeitungszentrum (IVZ) ... 72

1. Allgemeines ... 72
2. Einbeziehung der Rundfunkdatenschutzbeauftragten ... 73
3. ARD-ZDF-Vote ... 73
4. Neue technische Plattform für das Helpdesk-System "IVZRequest" ... 74

E. Datenschutz beim ARD-Hauptstadtstudio ... 74

F. Informationsmaßnahmen ... 75

G. Sonstiges ... 76

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR ... 76

II. Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern ... 77

III. Zusammenarbeit der datenschutzrechtlichen Aufsichtsbehörden nach der DSGVO 78

IV. Teilnahme an Fortbildungen und Veranstaltungen 79

Anlagen 79

1. Stellungnahme des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und DLR zur möglichen Einführung von Office 365 in der Europa-Cloud **(Anlage 1)**

2. Leitlinien zum Datenschutz in den öffentlich-rechtlichen Telemedien- und Social-Media-Angeboten der Rundfunkanstalten **(Anlage 2)**

3. Abkürzungsverzeichnis **(Anlage 3)**

Vorbemerkung

Am 25.05.2018 wird die EU-Datenschutz-Grundverordnung (DSGVO) in ganz Europa unmittelbare Rechtskraft entfalten. Davon ist auch der rbb betroffen. Zwar bleiben die grundlegenden Prinzipien des Datenschutzes, wie der Grundsatz der Zweckbindung, die Pflicht zur Rechtmäßigkeit der Verarbeitung, die Pflicht der Datensparsamkeit und die Transparenzplicht, bestehen. Jedoch kommen weitere Anforderungen hinzu. Vor allem die Dokumentationspflichten und die Informations- und Auskunftspflichten werden deutlich erhöht (s. B. I 1.1).

Die Identifikation der für den rbb notwendigen Maßnahmen zur Anpassung des Datenschutzmanagements an die DSGVO, die entsprechende Information und Schulung von Verantwortungsträgern, die Initiierung eines Projekts zur Umsetzung der notwendigen Maßnahmen und die Mitwirkung an dem Projekt haben einen großen Anteil meiner Tätigkeit innerhalb des Berichtszeitraums ausgemacht. Daneben waren für viele größere und kleinere IT-Projekte im rbb datenschutzrechtliche Vorabkontrollen und datenschutzrechtliche Unterweisungen durchzuführen. Ohne die Unterstützung des Mitarbeiters der Revision und stellvertretenden behördlichen Datenschutzbeauftragten Axel Kauffmann und meiner Kollegin im Sekretariat Sabine Kandetzki wäre die Arbeit kaum zu bewältigen gewesen. Ihnen beiden möchte ich an dieser Stelle herzlich danken. Auch dem Informationssicherheitsbeauftragten Michael Kalisch gebührt mein besonderer Dank. Er hat meine Arbeit mit seiner technischen Expertise und seinem Organisationsgeschick unterstützt. Gemeinsam haben wir das Bewusstsein für die Themen „Datenschutz und Datensicherheit" im rbb weiter vorangetrieben. Die Zusammenarbeit mit dem Personalrat verlief auch im Berichtszeitraum wieder angenehm und reibungslos. Ich kann mich darauf verlassen, dass der Personalrat einem neuen Projekt mit datenschutzrechtlicher Relevanz erst dann zustimmt, wenn mein positives Votum dazu vorliegt.

Vor dem Hintergrund, dass die Umsetzung der DSGVO im rbb noch lange nicht abgeschlossen sein wird und wir damit rechnen müssen, dass unter dem Regime der

DSGVO u. a. die Anzahl der Auskunftsersuchen gegenüber dem rbb erheblich ansteigt, werde ich in Zukunft wahrscheinlich eine größere personelle Unterstützung bei der Routinesachbearbeitung benötigen.

Dass die Datensicherheit in Zeiten zunehmender äußerer Bedrohung einen hohen Stellenwert hat, dürfte unmittelbar einleuchten. Aber auch der Datenschutz hat aus meiner Sicht nichts an Bedeutung verloren. Im Gegenteil. Ich schließe ich mich der Auffassung von Prof. Heribert Prantl an: „Der Exhibitionismus der Handy- und Internet-Gesellschaft kann kein Grund für das Vernachlässigen des Grundrechts auf Datenschutz sein. Denn: Wer sein Fenster aufmacht, erteilt nicht die Erlaubnis, bei ihm einzusteigen und die Wohnung auszuräumen. Zieht sich jemand halb aus, ist das nicht die Aufforderung an Dritte, ihn vollends zu entkleiden. Und wer im Großraumabteil der Bahn laut telefoniert, ist nicht damit einverstanden, dass der Personalchef ihn ausspioniert und Dossiers über seine Macken und Krankheiten anlegt. Im Übrigen sind die Handy-Posaunisten und die Internet-Exhibitionisten noch lange nicht „die Gesellschaft": Selbst dann, wenn Hunderttausende ausdrücklich und umfassend auf ihre Privatsphäre verzichteten, können sie das nicht mit Wirkung für Millionen anderer Menschen tun." (Prof. Dr. Heribert Prantl, DuD Datenschutz und Datensicherheit 2016, S. 347 ff.).

Förmliche Beanstandungen musste ich im Berichtszeitraum nicht aussprechen. Soweit es in Einzelfällen zu Verletzungen der Datenschutzbestimmungen gekommen ist, wurde meinen Empfehlungen in den Fachbereichen umgehend gefolgt.

Dieser Tätigkeitsbericht wird – wie die Vorgängerberichte - nach Erstattung gegenüber dem Rundfunkrat - im Online-Angebot des rbb veröffentlicht werden.

Er wird unter

http://www.rbb-Online.de/unternehmen/der_rbb/struktur/datenschutz/datenschutz_im_rbb.html

abrufbar sein.

A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg

I. Gesetzliche Grundlagen

Die Rechtsgrundlagen für die Datenschutzbeauftragte des rbb haben sich im Berichtszeitraum nicht verändert und werden sich wohl auch nach Wirksamwerden der DSGVO nicht ändern (s. B. III. 1.2).

Gemäß § 38 Abs. 1 rbb-Staatsvertrag (rbb-StV) bestellt der Rundfunkrat einen Beauftragten oder eine Beauftragte für den Datenschutz. Der oder die Beauftragte für den Datenschutz ist in Ausübung seines/ihres Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er/sie der Dienstaufsicht des Verwaltungsrates.

Gemäß Abs. 2 Satz 2 überwacht er/sie die Einhaltung der Datenschutzvorschriften des rbb-Staatsvertrags und anderer Vorschriften über den Datenschutz, soweit der rbb personenbezogene Daten zu eigenen, journalistisch-redaktionellen oder literarischen Zwecken verarbeitet.

Soweit eine Befugnis des oder der Beauftragten für den Datenschutz nach Abs. 2 Satz 1 nicht gegeben ist, obliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen beim rbb dem oder der Landesbeauftragten für den Datenschutz des Landes Berlin. Die Kontrolle erfolgt im Benehmen mit dem oder der Landesbeauftragten des Landes Brandenburg (Abs. 8).

Für die Sicherstellung des Datenschutzes im wirtschaftlich-administrativen Bereich ist beim rbb außerdem – wie bei allen Berliner Behörden und sonstigen öffentlich-rechtlichen Stellen – eine behördliche/ein behördlicher Datenschutzbeauftragte/r sowie jeweils eine Stellvertreterin/ein Stellvertreter schriftlich zu bestellen (§ 36 Abs. 1 rbb-Staatsvertrag i. V. m. § 19 a Berliner Datenschutzgesetz – BlnDSG).

II. Konkrete Situation

Auf seiner Sitzung am 03.09.2015 hat mich der Rundfunkrat gemäß § 38 Abs. 1 rbb-Staatsvertrag auf Vorschlag der ehemaligen Intendantin Frau Dagmar Reim für eine weitere Amtszeit von vier Jahren rückwirkend vom 01.07.2015 bis zum 30.06.2019 zur Beauftragten für den Datenschutz beim rbb bestellt. Parallel dazu hat Frau Reim für den gleichen Zeitraum meine Bestellung zur behördlichen Datenschutzbeauftragten im Sinne von § 19 a BlnDSG entsprechend verlängert. Meine Funktion als Datenschutzbeauftragte des rbb nehme ich nebenamtlich zu meiner Tätigkeit im Justitiariat wahr. Seit 01.04.2014 ist der Mitarbeiter der Revision, Axel Kauffmann, stellvertretender behördlicher Datenschutzbeauftragter. Herr Kauffmann vertritt mich in Abwesenheitsfällen. Bei größeren Projekten beziehe ich ihn von Anfang an mit ein, damit er jederzeit in der Lage ist, im Bedarfsfall für mich einzuspringen. Im Berichtszeitraum hat Herr Kauffmann auch wieder eine Reihe von Datenschutzschulungen übernommen (s. F.).

Zum 01.06.2017 hat Frau Sabine Kandetzki die Sekretariatsarbeit im Datenschutz von Frau Anja Hubert übernommen. Frau Kandetzki erledigt die Arbeit für den Datenschutz - wie zuvor Frau Hubert in der ehemaligen Direktion Recht und Unternehmensentwicklung - neben ihrer Tätigkeit im Sekretariat des Justitiariats.

Seit dem 01.07.2016 ist Michael Kalisch hauptamtlicher Informationssicherheitsbeauftragter (ISB). In meinem letzten Tätigkeitsbericht hatte ich kritisiert, dass die Funktion des ISB nicht als Stabsstelle mit unmittelbarer Anbindung an die Geschäftsleitung eingerichtet worden ist, wodurch seine unabhängige Stellung unterstrichen worden wäre, sondern der Stabsabteilung Organisation und Informationstechnik (OUI) innerhalb der Verwaltungsdirektion zugeordnet ist. Zwar kann ich konstatieren, dass Herr Kalisch entsprechend Tz. 4.1 Abs. 2 der Dienstanweisung zur Gewährleistung der Informationssicherheit vom 23.04.2014 seine Funktion fachlich unabhängig ausübt und sich um sämtliche Datenverarbeitungsprozesse im oder für den rbb kümmert. Jedoch ist gerade bei der Beurteilung von Vorhaben, die

in der OUI angesiedelt sind, z. B. die Einführung von Microsoft 365 (s. C III 2.), eine Interessenkollision nicht völlig ausgeschlossen. Überdies sollte der ISB keinerlei Aufgaben des operativen Geschäfts übernehmen, was zurzeit nicht strikt durchgehalten wird. Offenbar ist meiner Kritik inzwischen Rechnung getragen worden. Nach dem ab 1. Mai 2018 gültigen Organigramm ist Herr Kalisch dem Direktor für Produktion und Betrieb zugeordnet.

Für äußerst wichtig halte ich es – vor allem für dringende Anliegen -, dass es auch einen Stellvertreter für den ISB gibt, was bislang nicht der Fall ist.

Bei der Begleitung aller rbb-Projekte mit datenschutzrechtlicher Relevanz arbeite ich mit Herrn Kalisch eng zusammen. Darüber hinaus unterstützt er mich in vielen Einzelfragen mit seiner technischen Expertise. Die Schulungen zu Datenschutz und Informationssicherheit führen wir in der Regel gemeinsam durch (s. F.).

B. Entwicklung des Datenschutzrechts

I. Europa

1. Normen und Abkommen

1.1 EU-Datenschutz-Grundverordnung

Wie in meinem letzten Tätigkeitsbericht berichtet, erfolgte nach langen Verhandlungen im Dezember 2015 die europäische Einigung auf die EU-Datenschutz-Grundverordnung (DSGVO). Diese wird zu einer weitgehenden Vereinheitlichung des europäischen Datenschutzrechtes führen. Während bislang durch nationale Gesetzgebungen auf Grundlage der EU-Datenschutzrichtlinie erhebliche Unterschiede bestanden, wird die DSGVO ab 25.05.2018 direkt geltendes Recht in allen Mitgliedsstaaten sein. Alle nationalen Gesetze müssen entsprechend angepasst werden. All das, was die DSGVO regelt, ist als abschließend anzusehen, die entsprechenden nationalen Regelungen fallen grundsätzlich weg. Vom nationalen Gesetzgeber können im Wesentlichen nur noch Verfahrensfragen und Zuständigkeiten geregelt werden. Es gibt allerdings zwei Öffnungsklauseln, die dem nationalen Ge-

setzgeber Raum für eigene Regelungen lassen: Zum einen handelt es sich um die Öffnungsklausel zur Regelung des Medienprivilegs (Art. 85 DSGVO). Dabei geht es um den Auftrag für die Mitgliedstaaten, für den journalistischen Bereich angemessene Ausnahmeregelungen zum ansonsten strengen Datenschutzregime zu formulieren. Die zweite Öffnungsklausel betrifft die Regelung der Beschäftigtendatenverarbeitung (Art. 88 DSGVO). Für den rbb werden die Regelungsgegenstände im Rundfunkstaatsvertrag (RStV) und im neuen Berliner Datenschutzgesetz (BlnDSG nF) geregelt (s. III).

Die grundlegenden Prinzipien des Datenschutzes bleiben auch nach der DSGVO unangetastet. Jedoch kommen weitere Anforderungen hinzu. Das betrifft vor allem die Dokumentationspflichten und Betroffenenrechte. Die DSGVO sieht im Rahmen der Rechenschaftspflicht als zentrales Element vor, dass jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten (VVT) mit personenbezogenen Daten führt und die Verarbeitungstätigkeiten darin näher beschreibt. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (=Datenschutzfolgeabschätzung) durchführen. Eine weitere zentrale Anforderung der DSGVO ist darüber hinaus, dass die Betroffenen, deren personenbezogene Daten (außerhalb des journalistischen Bereichs) verarbeitet werden, noch detaillierter als bislang über diese Datenverarbeitung informiert werden müssen. Auch die Auskunftsrechte der Betroffenen sind erweitert worden. Danach muss der rbb zukünftig in der Lage sein, innerhalb kurzer Zeit über sämtliche Verarbeitungen von Daten einzelner Personen (z. B. Nutzer der rbb-Telemedienangebote oder Mitarbeiter des rbb) umfassend Auskunft zu erteilen. Schon bisher gilt das Prinzip der Datenvermeidung und Datensparsamkeit. Mit der Einführung der Prinzipien „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen“ (= Privacy by Design und Privacy by Default, Art. 25 DSGVO) werden nun ausdrücklich auch Anforderungen an die Produktentwicklung und –implementierung gestellt, um eine wirksame Umsetzung dieser Datenschutzgrundsätze zu erreichen.

1.2 ePrivacy-Verordnung

Am 10.01.2017 hat die Europäische Kommission einen Vorschlag für eine ePrivacy-Verordnung vorgelegt, die die bestehende Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (sog. ePrivacy-Richtlinie) ersetzen soll. Die neue Verordnung, die – wie die DSGVO - unmittelbar in allen Mitgliedstaaten gelten soll, wird Regelungen zur elektronischen Kommunikation enthalten und damit die DSGVO präzisieren und ergänzen. Der Anwendungsbereich der elektronischen Kommunikation ist sehr weit zu verstehen. Neben den Telemediendiensten und den klassischen Kommunikationsdiensten wie Telefonie und SMS fallen auch internetbasierte Kommunikationsdienste, insbesondere Messenger wie Skype oder WhatsApp, sog. OTT-Dienste (Over-the–Top-Dienste) darunter. Das EU-Parlament stimmte im Oktober 2017 den Beschlussempfehlungen des federführenden Innenausschusses (LIBE) zu. Eine zügige Einigung in den Trilogverhandlungen zwischen Europäischem Parlament, Europäischer Kommission und Ministerrat ist allerdings nicht in Sicht. Mit einem Inkrafttreten der ePrivacy-Verordnung wird frühestens Anfang 2019 gerechnet.

Für den rbb ist vor allem die zukünftige Regelung des Webtracking von Interesse. Wie die meisten anderen Website-Betreiber führt auch der rbb mit Hilfe verschiedener Auftragsverarbeiter Webtracking zur Webanalyse und Reichweitenmessung durch. Bisher gelten in diesem Bereich die Regelungen des Telemediengesetzes (TMG). Erlaubt sind danach pseudonyme Nutzungsprofile, die nur anonyme oder pseudonyme Daten enthalten, d. h. Daten, aus denen der Anbieter nicht die Identität des Nutzers ableiten kann. Personenbezogene Nutzungsprofile sind demgegenüber nur mit ausdrücklicher Einwilligung zulässig. Möglicherweise wird es hier zukünftig mit der ePrivacy-Verordnung eine Lockerung insofern geben, als es zukünftig nur noch ein Widerspruchsrecht gegen Nutzungsprofile für Werbezwecke, nicht mehr aber gegen solche für Zwecke der bedarfsgerechten Gestaltung der Website oder für Marktforschungszwecke geben wird.

Ursprünglich war geplant, dass die ePrivacy-Verordnung zeitgleich mit der DSGVO wirksam wird. Dieser Zeitplan kann – wie ausgeführt - nicht eingehalten werden. Für die Übergangszeit zwischen Wirksamwerden der DSGVO und dem Inkrafttreten der ePrivacy-Verordnung verbleibt es für die elektronische Kommunikation zunächst dabei, dass für diese nur die Spezialregeln der bisherigen ePrivacy-Richtlinie und der darauf basierenden nationalen Gesetze (TMG) fortgelten (Art. 95 DSGVO).

1.3 Privacy Shield

Der **EU-US Privacy Shield** (zu Deutsch: Datenschutzschild) ist ein Abkommen auf dem Gebiet des Datenschutzes, das 2015 bis 2016 zwischen der Europäischen Union und den USA ausgehandelt wurde. Es besteht aus einer Reihe von Zusicherungen der US-amerikanischen Bundesregierung und einem Beschluss der EU-Kommission. Die Kommission hat am 12.07.2016 beschlossen, dass die Vorgaben des Datenschutzschilds dem Datenschutzniveau der Europäischen Union entsprechen; damit kann das Abkommen angewendet werden. Das Übereinkommen regelt den Schutz personenbezogener Daten, die aus einem Mitgliedsstaat der Europäischen Union in die USA übertragen werden. Ein angemessenes Datenschutzniveau kann danach für US-Firmen unterstellt werden, die sich dem Privacy Shield unterworfen haben. Der Privacy Shield war notwendig geworden, nachdem der Europäische Gerichtshof im Oktober 2015 die bis dahin angewendete Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt hatte. Der Privacy Shield ist aus Datenschutzsicht hoch umstritten und ist auch bereits gerichtlich angefochten. Ob er der gerichtlichen Überprüfung standhält, ist stark zu bezweifeln. Zwar schafft er gegenüber dem Safe-Harbour-Abkommen verbesserte Datenschutzbedingungen. Es ist allerdings äußerst fraglich, ob diese ausreichend sind, um den Europäischen Standard zu gewährleisten. Die Bestimmungen sind zum Teil unscharf, vage und es werden Begriffe uneinheitlich verwendet. Vor diesem Hintergrund ist von einem Datentransfer in die USA ausschließlich auf der Basis des Privacy Shields unbedingt abzuraten.

Aber auch eine Rechtfertigung des Datentransfers in die USA auf Basis von sog. Standardvertragsklauseln ist datenschutzrechtlich mit einem gewissen Risiko behaftet. In 2001 hat die EU-Kommission durch Beschluss festgestellt, dass unter Verwendung der Standardvertragsklauseln eine Datenverarbeitung außerhalb des EWR-Raums grundsätzlich stattfinden kann. Dabei regeln die Vertragsparteien in den Standardvertragsklauseln u. a. ihre jeweiligen Verpflichtungen zur Einhaltung des Datenschutzes, zum Umgang mit Beschwerden von Betroffenen, zur Information über Anfragen Dritter einschließlich Behörden und zur Kontrolle durch die Aufsichtsbehörden. Mit Blick auf die Entwicklungen in den USA, insbesondere den Erkenntnissen zum Vorgehen der Geheimdienste, und nicht zuletzt auch im Hinblick auf das Vorgehen der Regierung von Donald Trump werden auch die Standardvertragsklauseln zunehmend hinterfragt. Auch hier findet derzeit eine gerichtliche Überprüfung vor den Gerichten in Irland statt.

2. Gerichtliche Entscheidungen

2.1. EuGH-Urteil zur Speicherung dynamischer IP-Adressen durch Website-Betreiber

Nach einem Urteil des Europäischen Gerichtshofs (EuGH) vom 19.10.2016 kann der Betreiber einer Website ein berechtigtes Interesse daran haben, bestimmte personenbezogene Daten der Nutzer zu speichern, um sich gegen Cyberattacken zu verteidigen. Damit hat der EuGH die sehr restriktive Regelung des deutschen Telemediengesetzes (TMG) gekippt, wonach Telemediendiensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden dürfen, soweit dies für die konkrete Nutzung der Website oder zu Abrechnungszwecken erforderlich ist.

Die Entscheidung legitimiert die Praxis der allermeisten Webseitenbetreiber – auch des rbb -, die aus Datensicherheitsgründen die IP-Adressen ihrer Nutzer für einige Zeit speichern. Zugleich hat der EuGH in seiner Entscheidung klargestellt, dass dynamische IP-Adressen für den Website-Betreiber personenbezogene Daten

darstellen, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, den Nutzer anhand der Zusatzinformationen, über die dessen Internetanbieter verfügt, bestimmen zu lassen. In Deutschland gibt es rechtliche Möglichkeiten, die es dem Anbieter von Online-Mediendiensten erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen von Internetzugangsanbietern zu erlangen und anschließend die Strafverfolgung einzuleiten. Der Websiteanbieter verfügt somit über Mittel, die vernünftigerweise eingesetzt werden können, um mit Hilfe Dritter den Nutzer anhand der gespeicherten IP-Adressen bestimmen zu lassen. Folgerichtig hat der Bundesgerichtshof (BGH) mit Urteil vom 16.05.2017 – in Fortführung der Entscheidung des EuGH - entschieden, dass die dynamische IP-Adresse für einen Website-Anbieter ein personenbezogenes Datum darstellt. § 15 TMG sei dahin auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich ist, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten der Nutzer bedarf.

2.2. EuGH-Urteil zur Haftungsfreistellung von WLAN-Anbietern

Mit Spannung wurde die Entscheidung des EuGH vom 15.09.2016 zur Reichweite der Access Provider-Privilegierung von WLAN-Anbietern erwartet. Im Grunde stand die europarechtliche Existenzberechtigung der von der deutschen Rechtsprechung entwickelten Störerhaftung von WLAN–Anbietern auf dem Spiel. Nach Auffassung des EuGH haftet der Zugangs-Provider gemäß Art. 12 I E-Commerce-RL nicht für übermittelte Informationen, wenn er die Übermittlung nicht veranlasst, den Adressaten der Übermittlung nicht ausgewählt und die übermittelten Informationen nicht ausgewählt und verändert hat. Deshalb bleiben Schadensersatzansprüche und auch die Beanspruchung diesbezüglicher Abmahn- und Gerichtskosten ausgeschlossen. Grundsätzlich nicht ausgeschlossen sind laut EuGH hingegen die Erstattung der Abmahn- und Gerichtskosten bezogen auf den gemäß Art. 12 Abs. 3 E-Commerce-RL explizit zugelassenen Unterlassungsanspruch. Dem Zugangs-Provider könne

grundsätzlich auch die Pflicht zur (identifizierenden) Passwortsicherung auferlegt werden.

Um auch die Gefahr der Abmahnkosten und der Passwortpflicht für Deutschland endgültig auszuschließen, hat der Bundestag am 30.06.2017 dem von der Bundesregierung am 05.04.2017 beschlossenen Entwurf für das Dritte Gesetz zur Änderung des TMG zugestimmt. Der Bundesrat hat den Gesetzentwurf am 22.09.2017 gebilligt. Das Gesetz ist am 13.10.2017 in Kraft getreten. Näheres s. II. 1.2

2.3 EuGH-Urteil zur Vorratsdatenspeicherung

Der EuGH hat sich mit seinem Urteil vom 21.12.2016 zum zweiten Mal gegen eine „allgemeine und unterschiedslose" Vorratsdatenspeicherung in der Europäischen Union ausgesprochen. Schon in seinem Urteil vom 08.04.2014 hat der EuGH erklärt, dass die von der Vorratsdatenspeicherung von Daten betroffenen Personen auf solche beschränkt werden müssen, die in irgendeiner Weise in einer schwere Straftat verwickelt sind oder deren auf Vorrat gespeicherten Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten. In der Entscheidung vom 15.09.2016 wiederholte das Gericht seinen Standpunkt, wonach eine allgemeine und unterschiedslose Vorratsspeicherung von Daten sämtlicher Verkehrs- und Standortdaten aller Telekommunikationsnutzer europarechtswidrig ist. Lediglich eine gezielte Vorratsspeicherung von Daten, die hinsichtlich der Kategorien der zu speichernden Daten der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist, sei zulässig.

In Deutschland sind Telekommunikationsanbieter auf der Grundlage eines neuen Gesetzes zur Vorratsdatenspeicherung seit Juli 2017 verpflichtet, Internet- und Telefonverkehrsdaten jedes Bürgers zehn Wochen lang zu speichern, also etwa die Informationen, wer wann mit wem telefoniert hat. Auch die Standortdaten von Handys müssen Firmen vier Wochen lang speichern. Einige wesentlichen Aspekte dieses Gesetzes dürften mit den Maßgaben des EuGH nicht vereinbar sein. Das

Oberverwaltungsgericht (OVG) NRW hat bereits aufgrund des Eilantrags des Providers Spacenet mit Beschluss vom 22.06.2017 dessen Pflicht zur Vorratsdatenspeicherung gestoppt. Der Beschluss ist unanfechtbar. Die Speicherpflicht sei in der Folge des EUGH-Urteils - jedenfalls in ihrer gegenwärtigen Ausgestaltung - nicht mit Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG vom 12.07.2002 vereinbar. In einer öffentlichen Mitteilung zur Speicherpflicht nach § 113b Telekommunikationsgesetz (TKG) hat die Bundesnetzagentur angekündigt, von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der Pflicht zur Vorratsdatenspeicherung einstweilen abzusehen. Vorerst drohen Anbietern von Telekommunikationsdiensten damit auch keine Bußgelder, wenn sie Verkehrs- und Inhaltsdaten nicht wie vorgeschrieben speichern. Das Bundesverfassungsgericht (BVerfG) hat indes mit Beschlüssen vom 26.03.2017 Eilanträge auf Erlass einer einstweiligen Anordnung gegen das Gesetz abgelehnt. Es hatte auch schon vor der EuGH-Entscheidung entsprechende Eilentscheidungen abgelehnt. Auch im Anschluss an die Entscheidung des EuGH stellen sich nach Auffassung des BVerfG Fragen, die nicht zur Klärung im Eilrechtsschutzverfahren geeignet sind.

II. Bund

1. Normen

1.1. Bundesdatenschutzgesetz nF

Zeitgleich mit der DSGVO wird das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (DS-RL) (DSAnpUG-EU) in Kraft treten. Dieses Gesetz bezweckt vor allem eine Anpassung des Bundesdatenschutzgesetzes (BDSG) an die DSGVO. Im neuen Bundesdatenschutzgesetz (BDSG nF) finden sich neben gemeinsamen Bestimmungen für öffentliche Stellen des Bundes und nicht-öffentliche Stellen unter anderem Durchführungsbestimmungen zur DSGVO. Das BDSG nF ist teilweise auf Zuspruch, zum Teil aber auch wegen etwaiger Kompetenzüberschreitungen des Bundesgesetzgebers, einer angeblich unangebrachten Absenkung des bisherigen Datenschutzniveaus und mangelnder Rechtssicherheit für die Datenschutz-

Praktiker auf Kritik gestoßen. Kritisiert werden speziell auch eine unangemessene Ausweitung der Videoüberwachung, eine unzureichende Ausgestaltung der Durchführungsbestimmungen zu besonderen Verarbeitungssituationen – u.a. im Beschäftigungskontext – sowie eine möglicherweise verfassungswidrige Beschränkung der Datenschutzaufsicht bei Berufsgeheimnisträgern.

Für den rbb sind im BDSG nF hauptsächlich die Regelungen zum Beschäftigungsdatenschutz in § 26 von Interesse. Denn gemäß § 36 Abs. 1 rbb-StV i.V.m. § 2 Abs. 2 BlnDSG gelten bislang für die Verarbeitung der Arbeitnehmerdaten sowie der Daten arbeitnehmerähnlicher Personen die Vorschriften im BDSG (§§ 31 bis 35, 39 und 43). Auch in dem Entwurf für das an die DSGVO angepasste Berliner Datenschutzgesetz (BerlDSG nF) wird wiederum auf die Vorschriften zum Beschäftigtendatenschutz im BDSG nF verwiesen (§ 18, s. III. 1.2).

Der maßgebliche § 26 BDSG nF enthält seinerseits materiell-rechtlich wenige Änderungen, allerdings einige begrüßenswerte Klarstellungen. Verantwortliche dürfen personenbezogene Daten von Arbeitnehmern und arbeitnehmerähnlichen Personen auf der Grundlage von § 26 Abs. 1 BDSG nF verarbeiten, wenn dies für einen der folgenden Zwecke erforderlich ist:

- Entscheidung über die Begründung eines Beschäftigungsverhältnisses;
- Durchführung des Beschäftigungsverhältnisses;
- Beendung des Beschäftigungsverhältnisses oder
- zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag oder einer Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten.

Neben den bereits aus dem bislang geltenden § 32 Abs. 1 BDSG bekannten Zwecken „Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses" sieht § 26 Abs. 1 BDSG nF also nun auch ausdrücklich die Verarbeitung für personalvertretungsrechtliche Zwecke vor. Aber auch die Datenverarbeitung durch Personalräte wird sich künftig an § 26 BDSG nF messen lassen müssen. Auch hier ist nach dem klaren Wortlaut von § 26 Abs. 1 Satz 1 BDSG nF eine Erforderlichkeitsprüfung vorzunehmen.

§ 26 Abs. 2 BDSG nF erlaubt die Verarbeitung personenbezogener Daten für Zwecke der Aufdeckung von Straftaten im Beschäftigungsverhältnis. Die Norm entspricht dem bisherigen § 32 I 2 BDSG. Auch nach der neuen Regelung ist eine Datenverarbeitung nur unter Zugrundelegung einer strengen Verhältnismäßigkeitsprüfung erlaubt. Zudem ist vor der Untersuchung in einer Dokumentation festzuhalten, welche tatsächlichen Anhaltspunkte diesen konkreten Straftatverdacht begründen. Die Datenverarbeitung zur Aufdeckung von Straftaten erfasst offene und versteckte Überwachungsmaßnahmen. Nach der Rechtsprechung des Bundesarbeitsgerichts (BAG) können auch jenseits der strafrechtlichen Relevanz bei schweren Verfehlungen der Arbeitnehmer heimliche Überwachungsmaßnahmen möglich sein (s. 2.1).

§ 26 Abs. 2 BDSG nF stellt erstmalig gesetzlich klar, dass eine Datenverarbeitung im Arbeitsverhältnis auf der Grundlage einer Einwilligung grundsätzlich möglich ist. Zudem regelt die Vorschrift, unter welchen Umständen Beschäftigte in die Verarbeitung ihrer personenbezogenen Daten durch den Arbeitgeber einwilligen können.

Ob eine Einwilligung zur Datenverarbeitung im Arbeitsverhältnis wegen der Anforderungen an die Freiwilligkeit überhaupt möglich ist, war bislang umstritten. Bei der Beurteilung der Freiwilligkeit der Einwilligung muss der Arbeitgeber vor allem die im Beschäftigungsverhältnis bestehende Abhängigkeit des Beschäftigten und die Umstände, unter denen die Einwilligung erteilt wurde, berücksichtigen. Dabei kann nicht nur die Art des verarbeiteten Datums oder die Frage, wie stark das informationelle Selbstbestimmungsrecht des Beschäftigten tangiert wurde, relevant sein, sondern auch der Zeitpunkt der Einwilligungserklärung. Als Beispiel wird in der Gesetzesbegründung genannt, dass der Beschäftigte im Vorfeld des Abschlusses eines Arbeitsvertrags eher einer Drucksituation ausgesetzt ist, die Einwilligung zu erteilen, als nach Abschluss des Vertrags. Die Gesetzesbegründung greift damit Bedenken aus der juristischen Literatur auf.

Absatz 2 Satz 2 formuliert Regelbeispiele, wann bei einer Einwilligung im Beschäftigungsverhältnis Freiwilligkeit vorliegen kann. So ist insbesondere dann von Frei-

willigkeit auszugehen, wenn der Beschäftigte durch die Verarbeitung seiner Daten einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder Arbeitgeber und Beschäftigter gleichlaufende Interessen verfolgen. Die Gewährung eines Vorteils liegt laut Gesetzesbegründung beispielsweise in der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder in der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen. Zu den gleichgelagerten Interessen können etwa die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste oder die Nutzung von Fotos für das Intranet zählen.

Als formelle Einwilligungsvoraussetzung sieht das BDSG nF grundsätzlich die Schriftform vor, um die Tragweite der Einwilligung zu verdeutlichen und damit das Persönlichkeitsrecht des Beschäftigten angemessen zu schützen. Damit soll ebenfalls die Nachweispflicht des Arbeitgebers i. S. d. Artikel 7 Absatz 1 DSGVO umgesetzt werden. Ferner ist der Arbeitgeber zur Aufklärung in Textform über den Zweck der Datenverarbeitung und den jederzeit möglichen Widerruf durch den Beschäftigten sowie dessen Folgen verpflichtet.

Die Verarbeitung besonderer Kategorien personenbezogener Daten von Beschäftigten für die Zwecke des Beschäftigungsverhältnisses ist in § 26 Abs. 3 BSDG nF geregelt. Nach Art. 9 Abs. 1 DSGVO sind dies besonders sensible Daten d.h. solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Ferner betrifft dies auch die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung. Die Verarbeitung solcher Daten für Zwecke des Beschäftigungsverhältnisses ist nach Art. 26 Abs. 3 Satz 1 BDSG nF zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist. Zudem darf kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Auch an die Freiwilligkeit einer Einwilligung sind bei besonderen Kategorien personenbezogener Daten nach der Gesetzesbegründung strenge Anforderungen zu stellen.

Neu ist die Klarstellung im Gesetz, dass Daten zum Zwecke des Beschäftigungsverhältnisses nicht nur erhoben werden dürfen, wenn eine gesetzliche Ermächtigungsgrundlage vorliegt, sondern auch dann, wenn sich dies aus einer Kollektivvereinbarung ergibt. Darunter sind Tarifverträge und Dienstvereinbarungen zu verstehen. Mit dieser Klarstellung wird ständige Rechtsprechung normiert. Beim Abschluss solcher Kollektivvereinbarungen haben die Verhandlungspartner die Vorgaben von Art. 88 Abs. 2 DSGVO zu beachten. Dienstvereinbarungen und andere Kollektivvereinbarungen zur Verarbeitung personenbezogener Daten von Beschäftigten müssen somit angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen. Insbesondere müssen sie entsprechende Regelungen im Hinblick auf die Transparenz der Verarbeitung enthalten. Die bestehenden Dienstvereinbarungen müssen anhand dieser neuen Rechtslage beurteilt und ggf. angepasst werden.

§ 26 Abs. 5 BDSG nF stellt klar, dass bei Verarbeitung personenbezogener Daten die in Art. 5 DSGVO festgelegten Datenschutzprinzipien beachtet und umgesetzt werden müssen. Diese betreffen die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Transparenz, der Zweckbindung, der Datenminimierung, der Richtigkeit, der Speicherbegrenzung, der Integrität und der Vertraulichkeit personenbezogener Daten. Demnach muss der Verantwortliche sicherstellen, dass die Verarbeitung in einer Weise erfolgt, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, sowie die in Art. 5 Abs. 2 DSGVO normierte Rechenschaftspflicht.

Diese Verpflichtung richtet sich sowohl an den Arbeitgeber, als auch an den Personalrat, die personenbezogene Daten von Beschäftigten verarbeiten.

§ 26 Abs. 7 BDSG nF sieht wie die alte Regelung vor, dass auch nicht-automatisierte bzw. nicht dateimäßige Verarbeitung personenbezogener Daten stets den Vorgaben von § 26 Abs. 1 bis 6 BDSG nF unterliegt. Typische Fälle für die

Anwendung dieser Vorschrift in der betrieblichen Praxis sind das Befragen oder Beobachten von Beschäftigten.

Für die Praxis ist noch als wichtig hervorzuheben, dass Arbeitgeber die Verarbeitung personenbezogener Daten von Arbeitnehmern und arbeitnehmerähnlichen Personen neben § 26 BDSG nF auch auf die allgemeinen Erlaubnisvorschriften der Verordnung stützen können, etwa auf Art. 6 und 9 DSGVO.

Als Rechtsgrundlage für die Verarbeitung der Daten freier Mitarbeiterinnen und Mitarbeiter kommen zukünftig ebenfalls Art. 6 und 9 DSGVO in Betracht.

Gemäß Art. 6 Abs. 1 DSGVO ist die Verarbeitung rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) die betroffene Person hat ihre Einwilligung zu der Verarbeitung gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrages erforderlich;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der rbb unterliegt;
d) (...)
e) (...)
f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen (...).

Es wäre wünschenswert, wenn der Beschäftigtendatenschutz zukünftig noch ausführlicher als bislang geregelt würde und man für die Klärung von schwierigen Rechtsfragen nicht ganz überwiegend auf das Studium der Rechtsprechung angewiesen wäre. Im Koalitionsvertrag von CDU, CSU und SPD vom 07.02.2018 ist „die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes, das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft", vorgesehen. Das lässt hoffen.

1.2 Telemediengesetz

Am 13.10.2017 ist das Dritte Gesetz zur Änderung des Telemediengesetzes (TMG) in Kraft getreten. Der deutsche Gesetzgeber versucht schon seit geraumer Zeit, die rechtlichen Grundlagen für eine Ausweitung von offenen WLAN-Hotspots in Deutschland zu schaffen. Die Vorgängerregelungen boten keine hinreichende Sicherheit für den Betreiber. Nunmehr scheint die Rechtslage aber sicher zu sein. An Flughäfen, in Hotels und auch in den Rundfunkanstalten – überall kann nun freies Internet gefahrlos angeboten werden. Trotzdem bleibt geistiges Eigentum angemessen geschützt: Rechteinhaber könnten von WLAN-Betreibern verlangen, einzelne, konkret benannte, Internetseiten zu sperren. Dies ist dann möglich, wenn über die Internetseiten ein Nutzer urheberrechtlich geschützte Inhalte illegal verbreitet hat. Das verhindert, dass eine Rechtsverletzung sich wiederholt. Vor- und außergerichtliche Kosten dürften dem WLAN-Betreiber aber auch in diesem Fall nicht in Rechnung gestellt werden. Diese Regelungen betreffen den rbb dann, wenn er anwesenden Gästen WLAN-Zugänge anbietet.

1.3 Netzwerkdurchsetzungsgesetz

Am 01.10.2017 ist das Netzwerkdurchsetzungsgesetz in Kraft getreten. Das Gesetz richtet sich gegen Hetze und gefälschte Meldungen (sog. Fake News) in sozialen Netzwerken. Das Gesetz gilt für Betreiber sozialer Netzwerke wie Facebook, Twitter und YouTube. Die Betreiber müssen offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden nach Eingang einer Beschwerde löschen oder sperren. Bei komplexen Fällen gilt eine Sieben-Tages-Frist, um über die Löschung oder Sperrung zu entscheiden. Bei wiederholten und systematischen Verstößen gegen das Gesetz droht ein empfindliches Bußgeld. Den Plattformbetreibern wird eine engmaschige Berichtspflicht zum Umgang mit rechtswidrigen Inhalten auferlegt.

Das Gesetz wurde im Vorfeld sehr kontrovers diskutiert. Reporter ohne Grenzen und andere Kritiker sprachen von einem „Schnellschuss“, der „das Grundrecht auf Presse- und Meinungsfreiheit massiv beschädigen könnte“. Entscheidungen über

die Rechtmäßigkeit von Beiträgen würden privatisiert, das Gesetz mache Soziale Netze zu Richtern über „Hate Speech".

Zwar ist das Regelungsziel der Eindämmung von Hetze und gefälschten Meldungen begrüßenswert. Die vorgeschriebenen Maßnahmen scheinen aber zur Erreichung dieses Zwecks nur bedingt tauglich. Außerdem schießt das Gesetz möglicherweise über das Ziel hinaus. So gibt es beispielsweise keine Clearingstelle für Beschwerden über voreilig gelöschte legale Inhalte, wie ursprünglich vom Bundesrat gefordert. Erfahrungen in der Anwendung des Gesetzes bleiben abzuwarten.

2. Gerichtliche Entscheidungen

2.1 Urteile des Bundesarbeitsgerichts zu verdeckten Maßnahmen gegenüber Arbeitnehmern

Im Berichtszeitraum hat das Bundesarbeitsgericht (BAG) mehrere Urteile zu verdeckten Ermittlungsmaßnahmen gegenüber Arbeitnehmern erlassen:

In seinem Urteil vom 22.09.2016 hat das BAG zur verdeckten Videoüberwachung von Arbeitnehmern mit Bezugnahme auf seine frühere Rechtsprechung folgende Grundsätze statuiert:

Eingriffe in das Recht der Arbeitnehmer am eigenen Bild durch verdeckte Videoüberwachung sind dann zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist.
Ein weiteres Urteil des BAG zur verdeckten Videoüberwachung ist schon am 20.10.2016 ergangen. Darin stellt das BAG klar, dass die Erhebung, Verarbeitung

oder Nutzung von personenbezogenen Daten zur Aufdeckung von Straftaten lediglich einen „einfachen" Verdacht im Sinne eines Anfangsverdachts voraussetzt, der über vage Anhaltspunkte und bloße Mutmaßungen hinausreichen muss. Der Verdacht muss sich in Bezug auf eine konkrete strafbare Handlung oder andere schwere Verfehlung zu Lasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern richten. Er darf sich einerseits nicht auf die allgemeine Mutmaßung beschränken, es könnten Straftaten begangen werden. Er muss sich andererseits nicht notwendig nur gegen einen einzelnen, bestimmten Arbeitnehmer richten. Auch im Hinblick auf die Möglichkeit einer weiteren Einschränkung des Kreises der Verdächtigen müssen weniger einschneidende Mittel als die verdeckte Videoüberwachung zuvor ausgeschöpft worden sein.

In einem weiteren Urteil des BAG zur verdeckten Observation eines Arbeitnehmers durch einen Detektiv wegen des Verdachts einer vorgetäuschten Erkrankung und Konkurrenztätigkeit vom 29.06.2017 hat das BAG erneut konstatiert, dass verdeckte Maßnahmen auch zur Aufdeckung schwerwiegender Arbeitspflichtverletzungen zulässig sein können.

Schließlich hat das BAG in seiner Entscheidung vom 27.07.2017 in der Konsequenz seiner vorherigen Rechtsprechung klargestellt, dass der Einsatz eines Software-Keyloggers (= eine Software, die alle Tastatureingaben protokolliert und regelmäßig Screenshots fertigt) nicht nach § 32 Abs. 1 BDSG erlaubt ist, wenn kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder anderen schwerwiegenden Pflichtverletzung besteht.

Der Gesetzgeber war verschiedentlichen Anregungen – trotz schon vorhandener anderslautender Rechtsprechung des BAG – nicht darin gefolgt, die Überwachungsbefugnis in § 26 Abs. 1 Satz 2 BDSG nF auch auf die Aufdeckung schwerer Vertragsverletzungen auszudehnen. Allerdings ist davon auszugehen, dass verdeckte Maßnahmen auch im Fall eines Verdachts auf schwere Vertragsverletzungen im Einklang mit der Rechtsprechung des BAG auch weiterhin möglich sind. Als Rechtsgrundlage kommt die allgemeine Regelung in § 26 Abs. 1 Satz 1 BDSG nF in Betracht.

2.2 Urteil des OLG Frankfurt a. M. vom 05.10.2017 zur Aufklärungspflicht bei Vertrieb von Smart-TV

Das Landgericht (LG) Frankfurt hatte mit Urteil vom 10.06.2016 entschieden, dass die Gerätehersteller aus wettbewerbsrechtlichen Gründen beim Inverkehrbringen eines Smart-TV ihren Kunden gegenüber verpflichtet sind, diese darüber zu informieren, dass durch den Anschluss des Smart-TV an das Internet möglicherweise Daten über sie erhoben werden, ohne dass zuvor eine entsprechende Zustimmung oder Information erteilt worden ist. Das Ziel dieses Urteils, dem Verbraucher einen weitreichenden Schutz einzuräumen, der schon beim Vertrieb von Smart-TV ansetzt, ist begrüßenswert. Denn mit dem Anschluss des Smart-TV an das Internet gibt der Nutzer seine Anonymität grundsätzlich auf. Ohne weiteres Zutun fließt zumindest seine IP-Adresse zu den Anbietern, um Zusatzangebote zu den Fernsehprogrammen bereitzustellen. Leider hat das Oberlandesgericht (OLG) Frankfurt a.M. mit Urteil vom 05.10.2017 die Entscheidung des LG Frankfurt aufgehoben.

III. Berlin/Brandenburg

1. Normen

1.1 21. Rundfunkänderungsstaatsvertrag

Wie unter I 1.1 ausgeführt, müssen die nationalen Gesetze innerhalb der EU an die DSGVO angepasst werden. Im 21. Rundfunkänderungsstaatsvertrag (RÄndStV), den die Ministerpräsidenten zwischen dem 05. und 18.12.2017 unterzeichnet haben, sind mehrere rundfunkrechtliche Staatsverträge an die DSGVO angepasst worden. Ein Schwerpunkt war dabei die Verankerung des Medienprivilegs. Schon bisher regeln verschiedene Vorschriften (z. B. § 41 BDSG, § 57 Rundfunkstaatsvertrag, RStV) die beschränkte Anwendbarkeit von Datenschutzrecht und Datenschutzaufsicht auf Medien und Presse. Dieses sog. Medienprivileg ist Ausfluss der Medien- und Pressefreiheit des Art. 5 Abs. 1 GG. Ein weiterer Regelungspunkt des 21. RÄndStV ist eine Änderung des Rundfunkstaatsvertrages, wonach Kooperationen des öffentlich-rechtlichen Rundfunks nicht mehr nach einer bloßen „Kann-Vorschrift" möglich sind, sondern ausdrücklich als Bestandteil des Auftrages gelten.

Nach Ratifizierung durch die 16 Landesparlamente wird der 21. RÄndStV zum 25.05.2018 in Kraft treten.

Neben den Vorschriften zum Medienprivileg im RÄndStV ist für den rbb weiterhin der rbb-Staatsvertrag in Verbindung mit dem Berliner Datenschutzgesetz (BlnDSG) maßgeblich. Zur Anpassung des BlnDSG an die DSGVO s. 1.2.

1.2 Berliner Datenschutzgesetz nF

Seit Dezember 2017 liegt der Entwurf zur Anpassung des BlnDSG und weiterer Gesetze an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vor. Art. 1 des Gesetzes enthält das BlnDSG n F. Eine Änderung des rbb-StV ist derzeit offenbar nicht vorgesehen.

Von besonderem Interesse sind §§ 18 und 19 des Entwurfs. Mit diesen Vorschriften werden die in der DSGVO enthaltenen Öffnungsklauseln zum Beschäftigtendatenschutz (§ 18) und zum Medienprivileg (§ 19) geschlossen.

In § 18 des Entwurfs wird - wie auch schon im derzeitigen BlnDSG - auf die Vorschriften zum Beschäftigtendatenschutz im BDSG nF verwiesen. (s.).

In § 19 wird das Medienprivileg für den gesamten Medienbereich in Berlin geregelt. Bei dem Inhalt dieser Norm handelt es sich im Wesentlichen um Regelungen, die vergleichbar schon jetzt in § 37 rbb-StV geregelt sind.

Zur Kontrollzuständigkeit für den rbb findet sich keine Regelung, so dass für die/den rbb-Datenschutzbeauftragte/n demnach weiterhin § 38 rbb-StV maßgeblich sein wird. Die Pflicht zur Bestellung einer betrieblichen Datenschutzbeauftragten als Verbindungsstelle zwischen Unternehmen und staatlicher Aufsichtsbehörde für den Verwaltungsbereich ergibt sich zukünftig unmittelbar aus Art. 37 EU DSVO.

Die Zeitplanung für das BlnDSG nF sieht vor, dass die Änderungen zeitgleich mit dem Wirksamwerden der DSGVO zum 25.05.2018 in Kraft treten sollen.

1.3 Verordnungen zur Durchführung des Meldegesetzes (DVO Meldegesetz)

Neben der einmaligen Übermittlung von Meldedaten aller volljährigen Personen von den Einwohnermeldeämtern an die Rundfunkanstalten gemäß § 14 Abs. 9 Rundfunkbeitragsstaatsvertrag (RBStV), die im Jahre 2013 und 2014 erstmalig stattgefunden hat und im Jahr 2018 wiederholt werden soll, findet auch eine regelmäßige Datenübermittlung von den Meldeämter an die Rundfunkanstalten zum Zwecke der Bestands- und Ersterfassung von beitragspflichtigen Personen statt (vgl. § 11 Abs. 4 Satz 4 RBStV). Die regelmäßige Meldedatenübermittlung erfolgt in Berlin und Brandenburg auf der Grundlage entsprechender Meldedatenübermittlungsverordnungen, die ihre Rechtsgrundlage bislang in den jeweiligen Landesmeldegesetzen hatten.

Da die Kompetenz für das Meldewesen von den Ländern auf den Bund übergegangen ist, ist am 01.11.2015 das Bundesmeldegesetz (BMG) in Kraft getreten. An diese neue Rechtslage mussten auch die Datenübermittlungsverordnungen der Länder angepasst werden.

<u>Für Berlin gilt:</u>

Die regelmäßige Datenübermittlung durch die Meldeämter an den rbb bzw. den Zentralen Beitragsservice für den rbb hat sich auf § 3 a der Verordnung zur Durchführung des Meldegesetzes (DVO-MeldeG), die gemäß § 26 des Gesetzes über das Berliner Meldewesens erlassen wurde, gestützt. Mit der Veröffentlichung im Gesetz- und Verordnungsblatt Berlin am 21.07.2016 ist das Berliner Ausführungsgesetz zum BMG in Kraft getreten, während damit zugleich das bisherige Meldegesetz außer Kraft getreten ist. Gemäß Art. 5 dieses Gesetzes wurde auch die DVO-MeldeG aufgehoben, wobei Art. 5 zusätzlich bestimmt hat, dass die §§ 3 bis 3b der

DVO-MeldeG bis zum Erlass einer neuen Verordnung, längstens jedoch bis zum 31.10.2017, weiter anzuwenden sind.

Zum 01.11.2017 ist die DVO-MeldeG durch die Verordnung zur Übermittlung von Meldedaten in Berlin (BlnMDÜV) ersetzt worden.

Für Brandenburg gilt:

Das Brandenburgische Meldegesetz in der Fassung vom 29.04.2015 enthält in § 11 eine Verordnungsermächtigung mit Verweis auf § 34 Abs. 1 und 3 BMG.

Auf dieser Grundlage regelt die Brandenburgische Meldedatenübermittlungsverordnung (MeldDÜV) in § 8 die Datenübermittlung an den rbb.

1.4 Rundfunkbeitragssatzung

Auf seiner Sitzung am 06.10.2016 hat der Rundfunkrat gemäß § 9 Abs. 2 Rundfunkbeitragsstaatsvertrag (RBStV) in der Fassung des 19. RÄndStV i. V. m. § 13 Abs. 2 Ziff. 4 rbb-StV die Satzung zur Änderung der Satzung des Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge vom 06.12.2012 i. d. F. vom 13.04.2014 beschlossen. Die Satzung ist an die neuen Bestimmungen des RBStV, die zum 01.01.2017 in Kraft getreten sind, angepasst. Da mit dem 19. RÄndStV bestimmte, bisher in der Satzung verankerte, Vorschriften auf die Ebene des RBStV gehoben wurden, war ihre Regelung in der Satzung entbehrlich geworden.

Inhaltlich sieht die neue Satzung zwei Änderungen vor: Zum einen wurde für die Rundfunkanstalten die Pflicht abgeschafft, an für jedermann zugänglichen Stellen Anzeigenformulare in Papierform auszulegen. Es hatte sich gezeigt, dass die Auslage der Formulare an diesen Stellen, insbesondere in Banken, aufgrund des Rückgangs des persönlichen Kundenverkehrs nicht mehr zeitgemäß ist. Es ist effizienter und bürgerfreundlicher, die Bürgerinnen und Bürger auf die Nutzung der Formulare im Internet zu verweisen bzw. ihnen diese auf Nachfrage kostenfrei in Papierform

zuzusenden. Zum anderen ist die bisherige Regelung gestrichen worden, wonach die Rundfunkanstalten erst dann Inkasso-Unternehmen beauftragten dürfen, nachdem der geschuldete Betrag durch die hoheitliche Vollstreckung nicht oder nicht vollständig beigetrieben werden konnte. Nun kann der „Mahnpfad" flexibler gestaltet werden. Zweck ist nicht ein breiter, pauschaler Einsatz von Inkassounternehmen. Vielmehr ist es jetzt möglich, bei bestimmten Gruppen von Beitragsschuldnern (insbesondere im Falle der Direktanmeldung) zunächst eine Klärung durch private Dienstleister herbeizuführen, bevor eine kostenintensive und für den Beitragsschuldner mit Zwangsmaßnahmen verbundene hoheitliche Vollstreckung eingeleitet wird. Dies entlastet nicht zuletzt die Vollstreckungsorgane, die sich in den letzten Jahren einer erheblichen Mehrbelastung durch beitragsrechtliche Vollstreckungsersuchen ausgesetzt sahen. Im Rahmen eines Normenkontrollverfahrens gemäß § 47 VwGO hat das Oberverwaltungsgericht (OVG) Berlin-Brandenburg die Rundfunkbeitragssatzung und auch den Wegfall des Vorrangs des Vollstreckungsverfahrens umfassend geprüft und für rechtmäßig erklärt (s. 2.1).

Geplant ist, zunächst ein Testverfahren „Inkasso vor Vollstreckung" durchzuführen. HR und SWR haben sich zur Durchführung eines solchen Tests bereiterklärt. Dabei soll die Zusammenarbeit mit verschiedenen Inkassounternehmen betrachtet werden. Das Projekt konnte aus vergaberechtlichen Gründen noch nicht gestartet werden.

2. Gerichtliche Entscheidungen

2.1 Urteil des Oberverwaltungsgerichts Berlin-Brandenburg vom 29.11.2017 zur Rechtmäßigkeit der Rundfunkbeitragssatzung

Im Rahmen eines Normenkontrollverfahrens gemäß § 47 VwGO hat das OVG Berlin-Brandenburg die Rundfunkbeitragssatzung umfassend geprüft und weder formelle noch materielle Mängel festgestellt. Im Urteil vom 29.11.2017 führt das OVG aus, dass insbesondere die Ermächtigungsgrundlage in § 9 Abs. 2 i. V. m.

§ 10 Abs. 7 Satz 2 des Rundfunkbeitragsstaatsvertrages (RBStV) nicht gegen höherrangiges Recht verstoße und auch eine hinreichende Grundlage für alle Regelungen der Satzung sei.

Zunächst hat das Gericht klargestellt, dass das Normenkontrollverfahren kein geeignetes Instrumentarium bietet, um den RBStV bzw. dessen Einzelregelungen einer umfassenden und den Verfassungsgerichten vorbehaltenen Rechtmäßigkeitskontrolle zu unterziehen. Der Senat hat sodann die Rechtmäßigkeit der in der Satzung geregelten Anzeigepflichten, der Beweislastregelungen, der Möglichkeit zur Datenerhebung bei öffentlichen und nicht-öffentlichen Stellen, der Verrechnungsregelung und der Übertragung einzelner Tätigkeiten im Zusammenhang mit dem Beitragseinzug bestätigt. Erfreulich sind aus meiner Sicht auch die Ausführungen des Gerichts zum Wegfall des Vorrangs hoheitlicher Vollstreckung vor dem Einsatz von Inkassounternehmen, die unter Bezugnahme auf die Beschlussvorlage für die 93. Sitzung des Rundfunkrates am 06.10.2016 darauf abstellen, dass mit dieser Änderung keineswegs ein breiter, pauschaler Einsatz von Inkassounternehmen ermöglicht, sondern der Mahnpfad lediglich flexibler gestaltet werde. Mit dieser Zielrichtung und so in der Praxis gehandhabt, bestünden gegen den Wegfall der Vorrangregelung der Verwaltungsvollstreckung vor der Einschaltung von Inkassounternehmen keine durchgreifenden rechtlichen Bedenken.

2.2 Zwei Beschlüsse des Verwaltungsgerichts Berlin zum presserechtlichen Auskunftsanspruch des rbb

Aufgrund meiner Tätigkeit für das Justitiariat weiß ich, dass die Durchsetzung von presserechtlichen Auskunftsansprüchen – gerade im Zusammenhang mit brisanten Themen – oft sehr mühsam ist. Oftmals stützen die Behörden (zu Unrecht) ihre Ablehnung auf ein angebliches Gebot zur Vertraulichkeit. Auch datenschutzrechtliche Argumente werden zur Abweisung entsprechender Auskunftsersuchen gerne vorgeschoben. Leider führt auch der Rechtsweg hier oftmals nicht weiter. Schwierigkeiten bereitet es immer wieder, die Gerichte von der Eilbedürftigkeit der Durchsetzung der Auskunftsansprüche zu überzeugen. Der Verweis auf das Hauptsacheverfahren durch die Gerichte hat schon des Öfteren dazu geführt, dass ein Thema

aufgrund des Aktualitätsverlustes schon erledigt war, bevor Monate oder gar Jahre später endlich die gerichtliche Entscheidung im Hauptsacheverfahren gefällt wurde.

Aus dieser Reihe an unerfreulichen Erfahrungen ragen zwei zugunsten des rbb ergangene Eilentscheidungen des Berliner Verwaltungsgerichts (VG Berlin) aus dem Jahr 2016 heraus:

Mit Eilbeschluss vom 17.11.2016 hat das VG Berlin dem rbb einen Auskunftsanspruch gegenüber der Humboldt-Universität zu Berlin über den Studienabschluss einer damaligen Kandidatin für das Amt der Bürgermeisterin eines Berliner Bezirks zugesprochen. Anspruchsgrundlage sind § 23, § 4 Abs. 1 Pressegesetz Berlin (PresseG Bln) bzw. § 9 a RStV. Danach sind Behörden verpflichtet, den Vertretern von Medien zur Erfüllung ihrer öffentlichen Aufgaben Auskünfte zu erteilen, bzw. haben Rundfunkveranstalter gegenüber Behörden ein Recht auf Auskunft. Ausschlussgründe nach § 23, § 4 Abs. 2 PresseG Bln oder § 9 a Abs. 1 Satz 2 RStV lagen nach Auffassung des Gerichts nicht vor. Insbesondere sei kein entgegenstehendes schutzwürdiges privates Interesse erkennbar. In Betracht komme das informationelle Selbstbestimmungsrecht der Politikerin nach Art. 1 und 2 Abs. 1 GG. Das Recht auf informationelle Selbstbestimmung sei jedoch nicht ausschließlich dem Betroffenen im Sinne einer absoluten und uneinschränkbaren Herrschaft über seine Daten zugeordnet. Der Einzelne müsse vielmehr Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Im Rahmen der Abwägung zwischen den grundrechtlich geschützten Gütern der Pressefreiheit, wie des informationellen Selbstbestimmungsrechts, sei vorliegend insbesondere einzustellen, dass zum einen mit den Auskünften, die sich auf den Bereich der erbrachten Studien- und Prüfungsleistungen der Politikerin beziehen, nur die Sozialsphäre als der am geringsten geschützte Teil des informationellen Selbstbestimmungsrechts betroffen ist. Zum anderen sei festzuhalten, dass sich die Politikerin bereits selbst im Rahmen ihrer Tätigkeit als Mitglied des Berliner Abgeordnetenhauses zu ihrem beruflichen Werdegang geäußert und damit diesen Lebensbereich nicht nur der öffentlichen Information, sondern auch der öffentlichen Nachfrage geöffnet habe. Auch datenschutzrechtliche Erwägungen nach § 6 a Abs. 5 Berliner Hochschulgesetz (BerlHG) könnten dem presserechtlichen Aus-

kunftsanspruch nicht entgegengehalten werden. Diese datenschutzrechtlichen Normen dienten lediglich der Einhaltung der gesetzlich vorgeschriebenen Informationswege durch ihre Adressaten, es ginge hierbei aber nicht um eine Einschränkung des Auskunftsanspruchs der Medien. Nach
§ 13 BlnDSG sei überdies die Datenübermittlung an u. a. landesunmittelbare Anstalten des öffentlichen Rechts zulässig, sofern eine Rechtsvorschrift - wofür hier die grundrechtlichen Güter der Presse- und Rundfunkfreiheit schützenden genannten Informationsnormen in Betracht kommen – dies erlauben.

Mit Eilbeschluss vom 26.01.2017 hat das VG Berlin dem rbb einen Auskunftsanspruch gegenüber dem Polizeipräsidenten von Berlin in Bezug auf die Durchführung der Überwachung der Fussilet-Moschee mit einer Observationskamera und Auswertung der Aufzeichnungen im Zusammenhang mit den Ermittlungen gegen den späteren Täter des Attentats am Breitscheidplatz Anis Amri zugesprochen. Die vom Polizeipräsidenten geltend gemachten Auskunftsverweigerungsrechte hat das Gericht nicht anerkannt. Die geltend gemachte Einwendung, dass durch die Auskunfterteilung die sachgerechte Durchführung eines schwebenden Verfahrens vereitelt, erschwert, verzögert oder gefährdet werden könnte, greife nicht. Diese Einwendung sei nur bei einer konkreten und gewichtigen Gefährdung eines schwebenden Verfahrens anzuerkennen, die hier nicht ersichtlich war. Es ergebe sich auch keine Gefahr aus der Offenlegung operativer Arbeitsweisen des Bundeskriminalamts oder der Bundesanwaltschaft.

2.3 Beschlussverfahren Freienvertretung ./. rbb

Wie schon in meinem letzten Tätigkeitsbericht erwähnt, besteht zwischen dem rbb und der Freienvertretung ein Dissens hinsichtlich der Reichweite ihres Anspruchs auf Auskunft über personenbezogene Daten der von ihnen vertretenen freien Mitarbeiterinnen und Mitarbeiter. Auf der Grundlage des Freienstatuts erhält die Freienvertretung von der Personalabteilung des rbb regelmäßig einen Grundbestand an Daten der freien Mitarbeiterinnen und Mitarbeiter. Soweit ein entsprechender Anspruch besteht, erhält sie auch personenbezogene bzw. –beziehbare Daten. In den Fällen, in denen das Freienstatut nicht ausdrücklich die Zurverfügungstellung per-

sonenbezogener oder –beziehbarer Daten vorschreibt, werden ihr pseudonymisierte Daten zur Verfügung gestellt, soweit dies zur Erfüllung ihrer Aufgaben nach dem Freienstatut erforderlich ist. Ein Anspruch auf weitere personenbezogene Daten steht der Freienvertretung aus meiner Sicht – wie im letzten Bericht erläutert - nach der derzeitigen Rechtslage nicht zu. Die Freienvertretung sieht sich durch die Verweigerung weiterer Daten in ihrer Arbeit behindert und hat am 06.04.2017 einen Antrag auf die Durchführung eines sog. Beschlussverfahrens zur Feststellung der Verpflichtung des rbb zur Auskunft über weitere Daten vor dem VG Berlin gestellt. Eine Entscheidung ist noch nicht ergangen. Zunächst wird die Frage der Zuständigkeit des Verwaltungsgerichts für Rechtsstreitigkeiten dieser Art geklärt werden müssen.

C. Datenschutz und Datensicherheit im rbb

I. Neue Regelwerke

1. Dienstanweisung zur Konfliktregulierung im rbb

Am 16.09.2016 haben sich die Geschäftsleitung und der Personalrat auf eine Dienstvereinbarung zur Konfliktregulierung im rbb geeinigt. Geregelt wird der Umgang mit sozialen Konflikten, Diskriminierung, sexueller Belästigung und Mobbing. In der Dienstvereinbarung werden als Anlaufstellen u.a. der Personalrat, die Frauenvertreterin, die/der Suchtbeauftragte, die Schwerbehindertenvertretung und die Konfliktberaterin/der Konfliktberater genannt. Die zuletzt genannte Position wurde neu geschaffen. Seit dem 01.04.2017 ist Frau Christiane Fackeldey zur Konfliktberaterin des rbb bestellt. Alle Anlaufstellen garantieren den Ratsuchenden Vertrauensschutz. Sie haben absolutes Stillschweigen über die Informationen, Vorkommnisse und persönlichen Daten, die sie in ihrer Beratungsarbeit erhalten, zu wahren. Bei der Formulierung der Dienstanweisung wurde ich nicht einbezogen. Allerdings muss ich mich immer wieder mit den Inhalten näher beschäftigen. Zum Beispiel spielen die Regelungen bei der Frage der Ausgestaltung eines anonymen Hinweisgebersystems eine Rolle. Näheres dazu s. unter IV. 7.

2. Dienstvereinbarung über die Nutzung mobiler Telekommunikationsgeräte

Am 30.11.2016 ist die neue Dienstanweisung über die Nutzung mobiler Telekommunikationsgeräte in Kraft getreten. Mit ihr wurde die Fassung vom 28.08.2006 abgelöst. Zugleich sind auch neue Nutzungsbedingungen für mobile Telekommunikationsgeräte in Kraft getreten.

An der Erarbeitung der Texte der Dienstvereinbarung und der Nutzungsbedingungen habe ich mich intensiv beteiligt.

Die Nutzer von individuell zugeordneten dienstlichen Telekommunikationsgeräten haben die Möglichkeit, gegen Zahlung einer monatlichen Pauschale diese Geräte in Deutschland und innerhalb Europas auch privat zu nutzen. Die Mitarbeiterinnen und Mitarbeiter sind zu einer kostenbewussten Nutzung angehalten. Konkrete Hinweise dazu und zu den erforderlichen Sicherheitsvorkehrungen finden sich in den Nutzungsbedingungen.

Beim Kosten-Controlling wird das Recht auf Datenschutz der Mitarbeiterinnen und Mitarbeiter gewahrt. Im Regelfall können die Kostenstellenverantwortlichen nur einen Gesamtrechnungsbetrag pro Vertrag sowie die Gesamtrechnungsbeträge pro Kostenstelle sehen. Nur wenn begründeter Anlass zu einer weitergehenden Prüfung der angefallenen Kosten besteht, können die Kostenstellenverantwortlichen mit Zustimmung der Datenschutzbeauftragten bei der OUI eine vollständige Auflistung der Verbindungsdaten für genau zu benennende Verträge anfordern und auswerten. Diese Praxis ist durch die ständige Rechtsprechung des Landesarbeitsgerichts (LAG) Berlin-Brandenburg gedeckt, wonach der Arbeitgeber bei Vorliegen eines legitimen Grundes unter bestimmten Voraussetzungen auch auf den von dem Arbeitnehmer auch privat genutzten dienstlichen E-Mail-Account zugreifen und die Verbindungsdaten auswerten darf.

3. Rahmendienstvereinbarung über elektronische Zutrittskontrolleinrichtungen und Videoüberwachungsanlagen

Bisher hatte sich der der rbb eher als „offenes Haus“ verstanden. Das lässt sich angesichts der größer gewordenen Bedrohungen von außen nicht mehr länger vertreten. Der rbb hat die Verantwortung, auf die wachsenden Sicherheitsbedürfnisse seiner Mitarbeiterinnen und Mitarbeiter, Mieter, Gäste und Dienstleister sowie auf die gestiegenen Sicherheitsrisiken in Europa zu reagieren. Seit Dezember 2016 liegt der Projektauftrag für ein technisches Sicherheitskonzept für Berlin und Potsdam vor. Ziele sind unter anderem die Sicherung der Gebäudezugänge und der sensiblen Bereiche mit elektronischem Zugangskontrollsystem und Videoüberwachungsanlagen, Sicherung des Betriebsgeländes und der Zufahrten mit elektronisch gesteuerten Schranken-, Tür- und Toranlagen sowie die nachvollziehbare Erfassung der Zutritte externer Dienstleister. Im April 2017 hat der rbb mit dem Personalrat eine Rahmendienstvereinbarung über elektronische Zutrittskontrolleinrichtungen und Videoüberwachungsanlagen abgeschlossen. An der Erarbeitung des Inhalts der Rahmenvereinbarung habe ich mitgewirkt. In der Dienstvereinbarung ist festgelegt, dass die Zutrittskontrolleinrichtungen durch den rbb nicht zur Arbeitszeiterfassung und nicht zur arbeitsrechtlichen Leistungs- und Verhaltenskontrolle genutzt werden. Außerdem sind darin die Voraussetzungen für die Einführung jeder einzelnen elektronischen Zutrittskontrolleinrichtung und die Installation jeder einzelnen Videoüberwachungskamera definiert.

4. Dienstanweisung IT-Nutzung

Im Juli 2017 hat die Geschäftsleitung die „Dienstanweisung für die Nutzung von Informationstechnik (IT)“ verabschiedet. Damit ist der rbb einer entsprechenden Empfehlung des Landesrechnungshofes von Berlin gefolgt. Die seit 01.09.2017 gültige Dienstanweisung regelt nun umfassend die Nutzung von Systemen der technikgestützten Informationsverarbeitung. Mit ihr wurde die bislang gültige „Dienstanweisung Internet und Mail“ abgelöst. Inhaltlich sind die IT-Regelungen den meisten Anwenderinnen und Anwendern im täglichen Umgang mit Systemen der

technikgestützten Informationsverarbeitung – auch dank der regelmäßig stattfindenden Schulungen zu Datenschutz und Informationssicherheit - vertraut. Der große Vorteil der neuen Dienstanweisung besteht in einer besseren Übersichtlichkeit für die Beschäftigten. Demnächst wird eine Evaluation der Dienstanweisung und Anpassung an die DSGVO erfolgen.

II. Projekte und Arbeitsgruppen

1. Projekt Umsetzung DSGVO

Kurz vor Wirksamwerden der DSGVO zeigt sich, dass im rbb - wie in den meisten anderen Unternehmen - längst noch nicht alle notwendigen Maßnahmen umgesetzt sind. Vieles hat sich aber schon getan:

Auf ARD-Ebene ist ein Umsetzungsprozess initiiert, da alle Häuser vor denselben Herausforderungen stehen. Im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) haben wir inzwischen eine Reihe von Dokumenten, z. B. das Formular für das Verarbeitungsverzeichnis und den Mustervertrag zur Auftragsverarbeitung sowie Factsheets zu einzelnen Themen der DSGVO, verabschiedet. Zusammen mit den Informationssicherheitsbeauftragten der Häuser planen wir derzeit, eine einheitliche Software für die Dokumentation der notwendigen Informationen zum Datenschutz und zur IT-Sicherheit anzuschaffen. In Abstimmung mit dem Netzwerk IT-Vorhaben soll über den Bereich Einkauf des rbb eine zentrale Softwarelösung beschafft werden, die das Informationsverarbeitungszentrum (IVZ) künftig für alle Rundfunkanstalten betreibt.

Mitte Februar 2018 fand zur Klärung der notwendigen Schritte der Umsetzung der DSGVO ein Workshop für die Informationssicherheitsbeauftragten und Datenschutzbeauftragten der Rundfunkanstalten beim MDR statt. Ergebnis des Workshops ist eine DSGVO-Roadmap mit einer detaillierten Beschreibung der notwendigen Schritte.

Da sich in diesem Zusammenhang für den rbb wie für alle anderen Rundfunkanstalten viele komplexe organisatorische Fragestellungen ergeben, die alle Direktionen des Hauses betreffen, hat die OUI im Auftrag der Intendantin Anfang 2018 ein Organisationsprojekt unter der Leitung einer Kollegin aus dem Bereich Projekte und Organisation gestartet. An dem Projekt wirken u.a. der ISB, der stellvertretende behördliche Datenschutzbeauftragte und ich mit. Die Projektgruppe ist derzeit dabei, die empfohlene Roadmap auf den rbb anzupassen.

In den ersten Sitzungen am 24.01. und 13.02.2018 hat die Projektgruppe ihren Projektauftrag definiert. Danach dient das Projekt der Ermittlung des Handlungsbedarfs, der sich aus den neuen gesetzlichen Anforderungen der DSGVO für den rbb ergibt, der Verankerung dieses ermittelten Handlungsbedarfs in einem Regelungsrahmen sowie der Umsetzung in der ersten Stufe.

2. Jour Fixe IT-Projekte

In regelmäßigen Terminen informiert die OUI die Mitglieder des Personalrats, die Schwerbehindertenvertretung und die Datenschutzbeauftragte in einem informellen Rahmen über geplante und laufende Projekte. Dieser Rahmen ermöglicht es, offen über Ideen und Probleme zu reden und Beteiligungsrechte zu einem möglichst frühen Zeitpunkt zu identifizieren. Im Berichtszeitraum fanden Termine am 13.06. und 12.12.2016 sowie 10.04. und 25.09.2017 statt.

Schwerpunkte der Sitzung am 13.06.2016 war das Vorhaben „Single Sign on für Windows/SAP“ und das Vorhaben „User Self-Service „Passwort zurücksetzen“ (s. III. 9.).

In der Sitzung am 12.12.2016 wurde im Wesentlichen über das Projekt “elektronische Zutrittskontrolleinrichtungen und Videoüberwachungsanlagen“ gesprochen (s. I. 3.). Herr Kauffmann hat in diesem Zusammenhang daran erinnert, dass die Revision schon im Jahr 2010 einen Prüfbericht zur Sicherheit der rbb-Serverräume erstellt hat, der nach wie vor nicht vollständig umgesetzt sei. In der Sitzung von 10.04.2017 stellte die OUI die laufenden Projekte vor, dabei insbesondere die

Einführung von MS Office 365 (s. III. 2.), sowie ein neues Druckerkonzept. In der Sitzung vom 25.09.2017 stellte sich die neue Usability-Beauftragte Frau Barbara Prasch vor und die OUI gab einen Überblick zum aktuellen Stand der Projekte.

3. Informationssicherheitskreis

Nach der Dienstanweisung zur Gewährleistung der Informationssicherheit wird der ISB durch den Informationssicherheitskreis (ISK) unterstützt. Der Kreis setzt sich aus Vertretern aller Direktionen und der Beschäftigtenvertretungen sowie der Datenschutzbeauftragten zusammen. Die Revision, das IVZ und das ARD-Hauptstadtstudio nehmen mit beratender Stimme ebenfalls an den Sitzungen des ISK teil.

Aufgaben des ISK sind insbesondere:

- Abstimmung und Entscheidung bei sicherheitskritischen Vorfällen und Entwicklungen,
- Konkretisierung der Informationssicherheitsziele

und

- Initiierung, Beauftragung und Verabschiedung sowie Überprüfung von Informationssicherheitskonzepten und Informationssicherheitsstandards.

Im Berichtszeitraum hat der ISK am 04.10.2016, am 22.05., 03.07., 04.09. und 22.11.2017 sowie 15.01.2018 getagt. Auf den Sitzungen hat uns der ISB regelmäßig über die aktuelle Sicherheitslage informiert. Weitere Themen waren u. a. Aufgaben und Struktur des ISK, Auftragsdatenverarbeitung, das **I**nformations **S**icherheits **M**anagement **S**ystem (ISMS), die Entsorgung alter Datenträger, die Erstellung von Informationssicherheitskonzepten, der geplante Probebetrieb zu MS Office 365 und MS Cloud, das neue Videokonferenzsystem der ARD, die DSGVO und die rbb-Webauftritte.

III. Aktuelle IT-Projekte

1. Umstieg auf das neue Betriebssystem Windows 10

Bislang lief auf den rund 4.000 rbb-PC-Arbeitsplätzen und -Notebooks das Betriebssystem Windows 7 des Herstellers Microsoft. Der rbb hatte Windows 7 ab 2012 eigeführt - jedoch ist dieses Betriebssystem schon wieder veraltet. Der Hersteller Microsoft bietet schon seit Januar 2015 keine neuen Funktionen im normalen Support mehr an. Nur noch bis Januar 2020 erhält der rbb Patches und Sicherheitsupdates. Danach hätte er ein Sicherheitsproblem im Betrieb gehabt. Deshalb hat sich der rbb für Migration auf Windows 10 entschieden.

Da Windows 10 in der ARD und beim rbb als Standard-Betriebssystem für Standard-Arbeitsplätze gesetzt ist, hat der ISB von der ARGE Rundfunk-Betriebstechnik GmbH (RBT), einer Gemeinschaftseinrichtung von acht ARD-Anstalten und dem ZDF, im Dezember 2017 ein Informationssicherheitskonzept für den rbb-Standard-Client erstellen lassen. Seit Anfang 2017 migriert der rbb auf Windows 10. Die Migration soll bis 2019 abgeschlossen sein.

2. Probebetrieb „MS Office 365“ in der Europa-Cloud

In meinem letzten Tätigkeitsbericht hatte ich noch darüber informiert, dass die Nutzung der Cloud eines externen Anbieters für Online-Speichermöglichkeiten beim rbb bislang generell verboten war. Allerdings hatte ich auch schon angemerkt, dass die Bedeutung von Cloud-Lösungen allgemein und auch im rbb stetig zunimmt.

Inzwischen hat uns bei diesem Thema die Normativität des Faktischen eingeholt:

Im rbb wächst der Bedarf, mit bzw. an Dokumenten im Team arbeiten zu können. Informationen und Dokumente sollen auf einfachem Weg mit Kolleginnen und Kollegen oder externen Akteuren „teilbar“ sein. Immer wichtiger ist es, auch von unterwegs bspw. mit dem Tablet an Dokumenten arbeiten zu können.

Die Plattform MS Office 365 von Microsoft kann diese neuen Anforderungen erfüllen. Im Zuge der ARD-Harmonisierungsbestrebungen haben die zuständigen ARD-Gremien daher beschlossen, zukünftig einheitlich MS Office 365 zu nutzen.

MS Office 365 ist eine Kombination aus zahlreichen Cloud-Diensten und bekannten Office-Applikationen. Zwar erfüllt Microsoft einen hohen Sicherheitsstandard für MS Office 365. Die Microsoft-Rechenzentren weisen diverse Zertifikate in Bezug auf Informationssicherheit und Datenschutz nach. Allerdings behält sich Microsoft bei der sog. Europa-Cloud explizit vor, Daten bei Bedarf (z. B. aus Performance- oder aus Supportgründen) in die USA zu verschieben. Die ursprünglichen Rechtsgrundlagen für die Speicherung von Daten auf Systemen unter US-amerikanischer Hoheit („Safe Harbor") hat der EuGH für ungültig erklärt. An der Nachfolgeregelung „EU–U.S-Privacy Shield" gibt es, wie bereits berichtet, aus Datenschutzsicht ebenfalls Kritik, denn diese Regelungen binden lediglich Unternehmen, die sich diesen Regeln unterwerfen und stellen keinen vollständigen Schutz gegen staatliche Eingriffe dar. Allerdings ist es nach DSGVO nicht rechtlich ausgeschlossen, die EU-Cloud von Microsoft zu nutzen. Dafür müssen sog. Standardvertragsklauseln vertraglich vereinbart werden.

Alternativ bietet Microsoft eine „Deutschland-Cloud" an, bei der sich das Rechenzentrum in Deutschland befindet. Der Zugriff auf die Daten erfolgt dabei durch die Firma T-Systems als Datentreuhänder. Dadurch soll der Zugriff unter Beachtung von deutschen/europäischen Datenschutz-Normen sichergestellt und insbesondere der Zugriff von Dritten unterbunden sein. Diesem erhöhten Schutz der Daten stehen erhöhte Lizenzkosten gegenüber. Außerdem sind nicht sämtliche Anforderungen in der Deutschland-Cloud abbildbar. Und schließlich: Recherchen haben ergeben, dass auch bei der Deutschland-Cloud nicht gewährleistet ist, dass keinerlei Daten den Europäischen Raum verlassen. Aus diesem Grund wurde diese Alternative inzwischen wieder verworfen.

Aus Sicht des AK DSB wird mit dem Umstieg auf MS Office 365 ein Paradigmenwechsel begangen. Im großen Umfang wird die Verarbeitung von Unternehmensdaten und personenbezogenen Daten in die Hände eines Dritten und in die Cloud gegeben. Dies ist mit datenschutzrechtlichen Risiken verbunden (s. Stellungnahme des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und DLR zur möglichen Einführung von Office 365 in der Europa-Cloud (Anlage 1).

Der rbb hat am 15.09.2017 einen Probebetrieb mit MS Office 365 in der EU-Cloud gestartet, an dem verschiedene Bereiche des rbb – u. a. die OUI und die Intendanz – teilnehmen. Der Probebetrieb fokussiert sich auf die Applikationen SharePoint, OneDrive for Business und Office pro Plus-Paket (Word, Excel, PowerPoint, OneNote etc.).

Ziele des Probebetriebs sind unter anderem:

- notwendige Betriebserfahrungen gewinnen,
- User-Feedback hinsichtlich Verwendbarkeit, Stärken und Schwächen der Plattform, Usability, Schulungsbedarf etc. erhalten,
- sinnvolle Applikations- und Funktionsumfänge testen,
- Klassifizierungen und Richtlinien für Dokumente erhalten und diese testen,
- notwendige Anpassungen für die IT-Nutzungsrichtlinien erfahren und
- ein Datenspeicherkonzept erarbeiten und prüfen.

Ausschlaggebend für meine Zustimmung zum Probebetrieb waren folgende Überlegungen:

Innerhalb des Probetriebs erhält der rbb die Möglichkeit, Erfahrungen in der Anwendung von MS Office 365 zu sammeln, die für die Festlegung der Rahmenbedingungen des Regelbetriebs sehr hilfreich sind. Das Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit der Daten ist laut Einschätzung des ISB angesichts der

von Microsoft gebotenen Sicherheitsmaßnahmen – auch in der EU-Cloud - akzeptabel. Sensible Dokumente werden zusätzlich manuell verschlüsselt. Besonders sensible Daten – z. B. Daten im Zusammenhang mit dem investigativen Journalismus – dürfen generell nicht in die Cloud gestellt werden. Mit der Entscheidung für die EU-Cloud im Probebetrieb präjudiziert sich der rbb nach Aussage des Projektverantwortlichen nicht für einen Regelbetrieb. Gegenüber der Geschäftsleitung habe ich die Erwartung geäußert, dass der rbb am Ende des Probebetriebs Ende August 2018 noch einmal sehr kritisch prüft, ob es der Mehrwert dieser technischen Lösung tatsächlich rechtfertigt, mit MS Office 365 in die Cloud zu gehen bzw. ob nicht – wie beim IVZ - eine Inhouse-Lösung (sog. on premise) vorzugswürdig ist. Eine andere Möglichkeit wäre eine Hybridlösung, bei der die Cloud wirklich nur in den Bereichen zum Einsatz kommt, wo sie wirklich zwingend erforderlich ist. Das Problem der Abhängigkeit von dem Unternehmen Microsoft, das die am 19.02.2018 im Ersten Fernsehprogramm ausgestrahlte rbb-Dokumentation „Das Microsoft-Dilemma" anschaulich vor Augen geführt hat, wäre freilich auch mit einer solchen Variante nicht gelöst. Aus dieser Abhängigkeit könnte nur der Umstieg auf eine gleichwertige „Open Source-Software" führen. Dies dürfte aber wohl schon wegen des Beschlusses, innerhalb der ARD einheitlich vorzugehen, keine realistische Alternative sein.

3. OpenMedia/Multimediales Redaktions- und Planungssystem (MRPS)

In meinen früheren Tätigkeitsberichten hatte ich darüber berichtet, dass der rbb für die Beitragserstellung seit 2013 eine gemeinsame Plattform für die Bereiche Hörfunk, Fernsehen und Online nutzt. Es handelt sich um das Redaktionssystem OpenMedia. Inzwischen ist dieses Redaktionssystem in fast allen Häusern der ARD installiert. Zum Start des Probebetriebs 2013 wurde eine Sicherheitsuntersuchung von der RBT durchgeführt. Ein Informationssicherheitskonzept wurde nicht erstellt. Der Probebetrieb ist immer wieder verlängert worden, da die Anbindung der Hörfunk-Schnittstellen komplexer war als gedacht.

2017 wurde die eigentlich schon zum Probebetrieb fällige Schutzbedarfsfeststellung für die im OpenMedia-System gespeicherten Inhalte vom ISB mit einem Mitarbeiter der Programmdirektion, dem Systemverantwortlichen und mir durchgeführt. Da die für OpenMedia verwendete Hardware schon seit 2011 im Einsatz ist, wurden Ersatzinvestitionen nötig. Dabei ist das OpenMedia-System aus den Erfahrungen neu aufgebaut worden. Für das neue System hat der Bereich Zentrale Systeme nun die Erstellung eines Sicherheitskonzepts bei der RBT in Auftrag gegeben.

4. Video Produktions Management System VPMS

Seit Ende 2016 findet im rbb durchgängig eine vernetzte filebasierte Fernsehproduktion im HDTV-Format statt. Der rbb hat sich für das Produkt "Video Production Management System" (VPMS) entschieden. Inzwischen arbeiten alle Redaktionen mit dem System. VPMS war bereits im Archiv des rbb und als Fernseh-CMS beim MDR, NDR, hr, RB, SWR und WDR im Einsatz. VPMS hat eine in der ARD bewährte Schnittstelle zum Redaktionssystem "OpenMedia", das der rbb als multimediales Redaktions- und Planungssystem einsetzt (s. 3.). Beim Aufbau des VPMS spielten Datenschutz und Datensicherheit leider keine Rolle. Ich war nicht eingebunden. Das wird jetzt gerade nachgeholt.

Durch Berichte über die weltweit zunehmende Zahl von Hackerangriffen und die damit verbundenen Schäden sensibilisiert, hat der Systembetreiber für VPMS das aus meiner Sicht längst fällige Informationssicherheitskonzept bei der RBT in Auftrag gegeben. Als ersten Baustein zur Erstellung eines Sicherheitskonzepts hat der ISB dafür zusammen mit einem Kollegen aus der Programdirektion, dem Systemverantwortlichen und mir eine Schutzbedarfsfeststellung für die Daten in VPMS durchgeführt. Das Sicherheitskonzept ist im Dezember erstellt worden. Aufgrund des Sicherheitskonzepts hat der ISB keine Empfehlung für den Regelbetrieb ausgesprochen, sondern eine Verlängerung des Probebetriebs empfohlen, bis die gröbsten Mängel behoben sind.

5. Unified Communication

Wechselnde Arbeitsplätze, wechselnde Arbeitsorte, wechselnde Aufgaben: Dies sind inzwischen die Arbeitsbedingungen für viele Mitarbeiterinnen und Mitarbeiter im rbb. Um diese Flexibilität zu unterstützen, hat der rbb testweise einen neuen Kommunikationsdienst, die „Unified Communication" (UC) eingeführt. Dabei werden verschiedene Kommunikationsmöglichkeiten auf einer einheitlichen Anwendungsumgebung gebündelt.

Im dritten Quartal 2018 ist eine Evaluation des Systems geplant, an der ich beteiligt werde. Auf Grundlage dieser Auswertung ist dann ein Antrag auf Probe- bzw. Regelbetrieb vorgesehen.
Im UC-Testbetrieb gibt es dieselben Leistungsmerkmale wie in der herkömmlichen Telefonanlage. Die Funktionen sind in der Dienstvereinbarung Telekommunikationsanlagenverbund beschrieben. Nutzerinnen und Nutzer können einige Funktionen bei Bedarf für einen einzelnen Anruf einschalten, mit Ende des Telefonats schaltet das System wieder auf den Standard zurück.

Der UC-Testbetrieb bietet darüber hinaus folgende weitere Leistungsmerkmale:

- **One number service:**
  Erreichbarkeit über die persönliche Festnetzrufnummer auch am Smartphone, ohne dass dem rbb Kosten entstehen,
- **Telefonie:**
  Auswahl, ob über PC, Smartphone oder klassischem Telefon telefoniert wird,
- **Telefonkonferenz:**
  Einfacher Aufbau von Sprachkonferenzen,
- **Videotelefonie:**
  Sofern eine Webcam vorhanden ist, kann mit einem einzelnen anderen Teilnehmer eine Videotelefonie geführt werden,
- **Web Collaboration:**
  Die eigene PC-Bildschirmoberfläche kann einem anderen UC-Nutzer angezeigt werden,

- **Istant Messaging:**
  Chat-Funktionen.

Inzwischen hat der Testbetrieb mit der Mittagsmagazin (MiMa)-Redaktion begonnen. Der Testbetrieb soll bis zum 31.12.2018 laufen.

6. HTTPS-Proxy

Die OUI beabsichtigt eine Erweiterung des bestehenden Proxy-Systems, die es möglich machen wird, auch über HTTPS (verschlüsselte Verbindung) abgerufene Inhalte auf Schadsoftware (Malware) zu überprüfen. Aktuell ist dies nur bei unverschlüsselten HTTP-Verbindungen möglich.

Ein Proxy ist ein Server, der als Vermittler zwischen dem rbb-Netz und dem Internet fungiert. Er nimmt Anfragen entgegen und schickt dann eine neue Anfrage mit seiner eigenen Adresse als Absender an den eigentlichen Zielserver. Auch die Antwort wird dann zunächst an den Proxy geschickt. Dieser kann die in ihr enthaltenen Nutzdaten z. B. auf einen schadhaften Code überprüfen und, wenn die Prüfung bestanden ist, als neues Paket dem Absender der Anfrage zukommen lassen.

Bei Verbindungen über den HTTPS-Proxy werden in Zukunft SSL/TLS-verschlüsselte Verbindungen aufgebrochen und automatisch auf Malware hin analysiert. Die Ergebnisse dieses Scans werden eine Woche lang gespeichert, damit es im Nachhinein noch möglich ist, Malware aufzuspüren, die vorher nicht korrekt erkannt wurde.

Ich habe der Einführung des HTTPS-Proxy zugestimmt.

Zwar ist ein Abfangen vor allem verschlüsselter Kommunikation grundsätzlich problematisch, aber die Gefahr durch Schadsoftware wird immer größer und gleichzeitig geht die Tendenz dahin, dass selbst eher unkritische Seiten (z. B. YouTube) standardmäßig SSL-verschlüsselt sind. Heute trifft das bereits auf ca. 50% des

HTTP-Traffics zu, weshalb ein solches Proxying wichtig ist, um die Systeme, Daten und Prozesse des rbb zu schützen.
Wichtig war mir bei der Entscheidung, dass sensible Kommunikation, wie z. B. Online-Banking, von der Entschlüsselung ausgenommen wird. Sämtliche Daten, die bei der Inspektion durch den Proxyserver anfallen, werden von den Administratoren ausschließlich zur Fehlerbehebung eingesehen und verwendet.

Das automatische Scannen der Kommunikation durch den rbb ist gemäß § 32 BDSG bei Arbeitnehmerinnen und Arbeitnehmern bzw. gemäß § 6 Abs. 1 BerlDSG bei freien Mitarbeiterinnen und Mitarbeitern grundsätzlich zulässig. Mit dem Abfangen von Kommunikation ist jedoch das Telekommunikationsgeheimnis der Mitarbeiterinnen und Mitarbeiter berührt. Im rbb ist die private Nutzung des Internets in geringem Umfang erlaubt. Allerdings haben diejenigen, die Internet und E-Mail beim rbb auch privat nutzen, eine Einverständniserklärung unterschrieben, mit der sie darin eingewilligt haben, dass die private Internet- und E-Mail-Nutzung wie die dienstliche behandelt wird. Davon umfasst ist dann auch die Einwilligung zum automatischen Scannen der privaten Internet-Nutzung. Dies setzt allerdings voraus, dass die Nutzer von dem Scannen überhaupt Kenntnis haben.

Deshalb habe ich gefordert, dass die Nutzer ausdrücklich auf das Scannen der unverschlüsselten und verschlüsselten Internet-Abrufe hingewiesen werden.

7. Notfall-App

Seit Ende 2016 wird auf allen dienstlichen iOS-Geräten im rbb die sog. Notfall-App zur Verfügung gestellt. Sie stellt Handlungshinweise und Telefonnummern der Verantwortlichen aus Programm, Produktion, Technik und Verwaltung und darüber hinaus auch von externen Verantwortungsträgern für den Notfall zur Verfügung. Bei den Telefonnummern handelt es sich zum Teil um nicht veröffentlichte Handynummern. Mit der Notfall-App wurde der bisherige Notfallplan, ein laminierter Ausdruck, der überall im Haus verteilt worden war, abgelöst. Die Notfall-App bietet zudem eine direkte Verlinkung auf die rbb24-Internet-Seite sowie zum Twitter-Kanal der Tagesschau. Der Betrieb der Notfall-App obliegt der OUI, die Redaktion liegt wie

bisher beim „Aktuellen Tisch". Alle rbb-Mitarbeiter mit Dienstgeräten haben lesenden Zugriff auf die App. Angesichts der in der App enthaltenen unveröffentlichten Kontaktdaten der leitenden Mitarbeiterinnen und Mitarbeiter und der externen Ansprechpartner hatte ich im Vorfeld die Frage gestellt, ob es wirklich erforderlich sei, dass jeder Nutzer eines dienstlichen iOS-Gerätes die Notfall-App auf seinem Gerät hat. Darauf haben mir die Verantwortlichen geantwortet, dass die Daten laut Einschätzung des ISB auf dem Gerät sicherer abgelegt seien, als auf den laminierten Ausdrucken. Eine unterschiedliche Konfiguration der Dienstgeräte (mit bzw. ohne App) würde einen unverhältnismäßigen Pflegeaufwand bedeuten. Diese Argumentation habe ich akzeptiert, da es sich um dienstliche Kontaktdaten handelt und der Kreis der Nutzer dienstlicher IOS-Geräte überschaubar ist.

8. Software-Lizenz-Management-System „Snow Software"

Ende 2016 hat der rbb das Software-Lizenz-Management-System „Snow Software" eingeführt. Bei der Snow-Software handelt es sich um eine Lizenzmanagement-Software für Softwarelizenzen, welche einerseits die lizenzpflichtigen Softwareinstallationen auf Clientcomputer und auf Server inventarisiert und andererseits die Softwarekäufe mit ihren Nutzungsrechten bzw. Nutzungsbedingungen in dem System abbildet. Dabei ist es die Aufgabe, mit Hilfe der Snow-Software eine Lizenzbilanz zu erstellen und Softwarebedarfe abzubilden. In einer zentralen Datenbank werden die Softwareinstallationen sowie beschaffte Softwarelizenzen gespeichert. Der sog. Client-Agent liefert lizenzrelevante Daten. Dazu zählen alle Hardware-Informationen, Softwareinstallations- und Betriebssystemdaten wie Hersteller, Patch Level, Lizenz Key, Computername, Zeitzone und Installationsverzeichnis. Mit einer Historie von neunzig Tagen werden für diejenigen Benutzer-Accounts, die sich an einem Rechner angemeldet haben, dokumentiert, welche Software ausgeführt wurde, wie oft und wann die Anwendung zuletzt gestartet und wieviel Zeit sie insgesamt genutzt wurde.

Eine Schnittstelle zum E-Mail-System Lotus Notes ermöglicht dem Snow Server einen automatischen Versand von E-Mails für Alarmmeldungen oder Lizenzberichte an den Systemverantwortlichen und den Lizenzmanager der OUI.

Durch die Anbindung zum Active Directory (AD) identifiziert Snow nicht inventarisierte Server und Computer. Dabei überträgt die AD die Server- bzw. Computer-Namen in die Snow-Datenbank, damit OUI prüfen kann, ob alle Systeme vollständig inventarisiert sind.

Es gibt ein abgestuftes Berechtigungskonzept für die Nutzer dieser Software. Die beiden Hauptnutzer erhalten nur anonymisierte Darstellungen für das Lizenzmanagement. Lediglich zwei Personen erhalten auch Zugriff auf personenbezogene Informationen, die es ihnen ermöglichen, Rücksprache mit Nutzern von Software zum tatsächlichen Bedarf zu halten.

Der Einsatz eines Lizenz-Management-Systems liegt im berechtigten Interesse des rbb. Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Arbeitnehmerinnen und Arbeitnehmer sowie der arbeitnehmerähnlichen Mitarbeiterinnen und Mitarbeiter ist § 2 Abs. 2 BlnDSG i. V. m. § 32 Abs. 1 Satz 1 BDSG. Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten aller anderen freien Mitarbeiterinnen und Mitarbeiter ist § 6 Abs. 1 Satz 2 BlnDSG.

Auf der Basis des vom ISB vorgelegten Informationssicherheitskonzepts konnte ich der Einführung der Software zustimmen. Allerdings habe ich den Betreiber des Systems gebeten, im Sinne der Transparenz sämtliche betroffenen Nutzerinnen und Nutzer über den Einsatz von Snow zu informieren – z. B. durch eine entsprechende Meldung im Intranet.

9. ASPR – Passwort Reset Manager

Der rbb beabsichtigt die Einführung einer Self-Service-Lösung für das Passwort-Management (das Zurücksetzen der Passwörter). Dabei handelt es sich um eine

Web-Anwendung, die auf Standardkomponenten basiert und sowohl unterschiedliche Verfahren für den Passwort-Reset zulässt, als auch für verschiedene Zielsysteme Passwörter zurücksetzen kann. Der Zugriff auf die Anwendung erfolgt mit jedem Standard-Web-Browser über eine gesicherte HTTPS-Verbindung. Im Fall der Pflege der Benutzerdaten oder für die Mitarbeiter der OUI, die mit dem System arbeiten, erfolgt die Autorisierung mit Benutzerkürzel und Passwort der AD. Zentraler Prozess des Systems ist der Passwort-Reset. Für diesen Prozess kommt der Authentisierung des Benutzers besondere Bedeutung zu. Es wurden zwei Verfahren festgelegt, die der Benutzer alternativ einsetzen kann, um das Passwort zurückzusetzen: Ein Freischaltcode, den der Benutzer per SMS oder Email erhält, und hinterlegtes Wissen (durch die richtige Beantwortung von hinterlegten Fragen kann der Benutzer ebenfalls das Passwort neu setzen). Um die Benutzerinformationen wie Handy-Nummer oder E-Mail-Adresse sowie die Antworten auf die Fragen zu hinterlegen, gibt es die Funktionen der Datenpflege mit der Bezeichnung „Stammdaten bzw. Wissen hinterlegen". Für die Kolleginnen und Kollegen vom IT-Service gibt es unter der Funktion „Helpdesk-Bereich" die Möglichkeit, das Passwort auch am Telefon zurückzusetzen, wenn der Anrufer eine hinterlegte Frage richtig beantwortet. Es ist technisch sichergestellt, dass jeder Benutzer nur in der Lage ist, seine persönlichen Daten zu bearbeiten. Ein Zugriff auf die Daten Dritter ist auch für den IT-Service und die Administratoren nicht vorgesehen. Lediglich beim Passwortwechsel kann ein Mitarbeiter des IT-Services nach korrekter Beantwortung einer Kontrollfrage ein Passwort für einen Benutzer neu setzen. Bei dem Passwort-Reset unter Mitwirkung des IT-Service-Mitarbeiters muss sich der Benutzer im Anschluss gleich ein neues Passwort vergeben, welches der Kollege aus dem IT-Service nicht kennt. Zudem ist das Frage-/Antwort-Paar, mit dem sich der Benutzer des Passwort-Reset beim IT-Service-Kollegen autorisiert hat, verfallen. Die Antwort kann also nicht für einen weiteren Passwort-Reset verwendet werden. Auf der Basis des vom ISB erstellten Informationssicherheitskonzeptes konnte ich dem Probebetrieb im September 2017 zustimmen. Der Probebetrieb für den ASPR Passwort Reset Manager läuft seit dem 01.12.2017 – zunächst ausschließlich in der OUI. Parallel prüft die neue Usability-Beraterin Barbara Prasch die Webanwendung in Hinblick auf Usability und Barrierefreiheit.

10. Neues Fuhrparkmanagementsystem

Im Bereich Fuhrparkservice wird derzeit für die Disposition der dort zu disponierenden Fahrzeuge eine technisch veraltete Software, die auch nicht mehr sämtlichen fachlichen Anforderungen genügt, genutzt. Es besteht daher der Bedarf, diese durch ein Fuhrparkmanagementsystem zu ersetzen, das den aktuellen fachlichen Anforderungen entspricht, sowie zukunftsfähig, d.h. auch erweiter- und skalierbar, ist und technisch den IT-Anforderungen sowie den Sicherheitsanforderungen des rbb entspricht. Fachlich soll das künftige System die bisherige Disposition als auch künftig eine umfassende Verwaltung der Fahrzeuge und Fahrer leisten.

Der Personalrat hat dem Antrag auf Test- und Probebetrieb am 05.07.2017 zugestimmt. Vereinbart ist, dass ich vor Inbetriebnahme eine datenschutzrechtliche Vorabkontrolle nach § 5 Abs. 3 Satz 2 BlnDSG durchführe. Dazu haben bereits Gespräche mit mir stattgefunden, die erforderlichen Dokumente für die Vorabkontrolle sind in Arbeit. Test- und Probebetrieb sollten ursprünglich Mitte Juli 2017 starten. Inzwischen hat sich der Terminplan verschoben. Die Aufnahme des Test- und Probebetriebs ist nun für das Frühjahr 2018 geplant.

11. Neues Materialdispositionssystem „Easyjob“

Seit einiger Zeit testet der rbb das Materialdispositionssystem „Easyjob“. Dabei handelt es sich um ein Materialdispositionssystem/Warenwirtschaftssystem für Sachmittel, welches bereits in anderen ARD-Anstalten eingesetzt wird. Mit Easyjob sollen der Bestand und die Ein- und Ausgänge von technischem Equipment der Bereiche Audioproduktion, Mobile Technik und EB-Lager erfasst werden. Ende 2016 hat der ISB in einem vorläufigen Informationssicherheitskonzept beschrieben, welche Maßnahmen zur Gewährleistung der Datensicherheit ergriffen werden müssen (gesicherter Login, geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern, Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung, Protokollierung am Server etc.). Auf dieser Grundlage konnte ich dem Testbetrieb, mit einem System, das sich noch im Aufbau befindet, aber schon mit Echtdaten arbeitet, zustimmen.

IV. Beschäftigtendatenschutz

1. Umsetzung der SAP-Dienstvereinbarungen

In meinen früheren Tätigkeitsberichten hatte ich wiederholt moniert, dass die in den SAP-Dienstvereinbarungen festgelegten Löschfristen für personenbezogene Daten bislang nicht umgesetzt waren. Grund für die Unterlassung, die auch einen Verstoß gegen das Gebot der Datensparsamkeit darstellt, waren technische Schwierigkeiten, da durch das Löschen die Konsistenz der Datenbank gefährdet werden kann. Diese Schwierigkeiten konnten in Zusammenarbeit mit SAP inzwischen teilweise gelöst werden. Am 06.12.2017 wurden alle nicht mehr benötigten Abwesenheiten (Urlaub, Krankheit) gemäß den Festlegungen in den Dienstvereinbarungen gelöscht. Weitere nicht mehr benötigten Personaldaten werden nun nach und nach ebenfalls gelöscht. Dabei wird der Löschvorgang nach dem Vier-Augenprinzip durchgeführt. Ein Kollege/eine Kollegin aus der OUI bzw. dem IVZ stößt die Selektion der zu löschenden Daten an, die anschließend von einer Mitarbeiterin/einem Mitarbeiter der entsprechenden Fachabteilung (z. B. Personalabteilung) gelöscht werden kann.

2. Versand elektronischer Gehaltsabrechnungen

In meinem letztjährigen Tätigkeitsbericht habe ich über eine kleine Arbeitsgruppe aus Vertretern der Personalabteilung, des IVZ, der OUI, der Revision, dem ISB und mir berichtet, die ein Konzept für die Versendung von elektronischen Gehaltsabrechnungen erarbeitet hat. Im Sommer 2017 haben wir das Konzept dem Personalrat vorgestellt. Dabei wurde deutlich, dass die Versendung der Gehaltsabrechnungen per verschlüsselter E-Mail an den dienstlichen Mail-Account nur infrage kommt, wenn auch der Ausdruck der Abrechnung im rbb sicher ist. Viele Kolleginnen und Kollegen verfügen jedoch nicht über einen eigenen Drucker, sondern sind auf die Nutzung eines Netzwerkdruckers angewiesen. Um den nächstgelegenen Netzwerkdrucker zu erreichen, müssen oftmals lange Wege zurückgelegt werden. In der Zwischenzeit können Unbefugte den Ausdruck aus dem Drucker entfernen. Ich habe mich dafür ausgesprochen, den Probebetrieb für den Versand elektronischer Ge-

haltsabrechnungen bis zur Erarbeitung eines neuen Druckerkonzepts zurückzustellen. So wird nun verfahren.

3. Elektronisches Firmenticket

Das rbb-Firmenticket ist eine personengebundene Zeitkarte für Fahrten mit öffentlichen Verkehrsmitteln der im Verkehrsverbund Berlin-Brandenburg (VBB) zusammenwirkenden Verkehrsunternehmen. Dazu gehören unter anderem die Berliner Verkehrsbetriebe (BVG), die S-Bahn Berlin GmbH, die ViP Verkehrsbetriebe Potsdam GmbH sowie die regiobus Potsdam Mittelbark GmbH, welche die Firmentickets für die Mitarbeiterinnen und Mitarbeiter des rbb bereitstellt. Das rbb-Firmenticket beinhaltet grundsätzlich dieselben Leistungen wie reguläre Monatskarten der VBB-Unternehmen, d.h. die Nutzung der Busse, Bahnen und Fähren der VBB-Unternehmen. Bisher gab es die Firmentickets in Form von Papier, bestehend aus einer Trägerkarte und jeweils 12 einzelnen Monatsabschnitten. Seit Frühsommer 2017 gibt es den elektronischen Fahrausweis. Dies erfordert bei Antragstellung die Abgabe eines elektronischen Lichtbildes inklusive Zustimmung zu der Speicherung des Bildes bei der regiobus GmbH. Dies hat zwei Vorteile: Bei Verlust kann die Karte kurzfristig gesperrt und sofort neu ausgestellt werden. Bei Verlängerung wird kein neues Bild benötigt. Die Personalabteilung ist in dieser Sache frühzeitig auf mich zugekommen. Ich habe keine Einwände gegen die Einholung eines digitalen Lichtbildes und die Übermittlung an die regiobus GmbH zur Erstellung eines elektronischen Fahrausweises. Allerdings habe ich gefordert, dass die Übermittlung der Fotos auf sicherem Weg erfolgt. Dazu hat die Personalabteilung mit Unterstützung des ISB folgende Lösung gefunden: Die zuständigen Mitarbeiter der Personalabteilung laden die Fotos in die vom IVZ betriebene ARD/ZDF-Box-Cloud. Außerdem leitet sie der Firma regiobus GmbH per Mail einen Link zu, wobei genau festgelegt werden kann, welche Bilder die Firma aus der Cloud sieht und wie lange darauf zugegriffen werden kann.

4. Bewerbermanagementsystem Umantis

Wie in meinem letzten Tätigkeitsbericht erwähnt, hat der rbb im Herbst 2016 mit meiner Zustimmung den Probebetrieb des elektronischen Bewerbermanagementsystems Umantis aufgenommen. Seitdem werden sämtliche Bewerbungen über das neue elektronische System abgewickelt. Die Bewerbung in Papierform ist nach wie vor möglich. In diesem Fall scannen die Sachbearbeiter der Personalabteilung die Papierunterlagen und speichern die Daten im System, um sie anschließend – wie die Online-Bewerbungen – elektronisch weiterzuverarbeiten. Das Hosting des Systems findet in einem zertifizierten Rechenzentrum in Deutschland statt. Der rbb hat die in diesen Fällen übliche Vereinbarung zur Auftragsdatenverarbeitung mit dem Vertragspartner abgeschlossen. Die Datenübertragung und -speicherung erfolgen verschlüsselt. Das Bewerbungsformular enthält einen deutlichen Datenschutzhinweis. Die Nutzung des Systems kann nur mittels Authentifizierung erfolgen. Bei meiner Vorabkontrolle des Systems hatte ich außerdem Wert auf ein differenziertes Berechtigungskonzept gelegt. Die Rollen der Systemnutzung und der Administration sind getrennt. Vier Monate nach Abschluss des Bewerbungsverfahrens werden alle Bewerbungen der jeweiligen Ausschreibung von den Administratoren gelöscht. Dies geschieht aus technischen Gründen leider nicht automatisch, sondern manuell. Vom Löschvorgang ausgeschlossen sind lediglich statistische Informationen. Die Administratoren sind im Löschen der Daten geschult. Die Anmeldung an das System mit Zugriffsrechten auf Bewerbungen anderer Personen ist ausschließlich auf Endgeräten möglich, die über eine rbb-IP-Adresse verfügen. Damit ist ein Zugang zu Bewerberdaten nur auf Rechnern innerhalb des rbb sowie auf rbb-iPads sowie rbb-Notebooks unter Verwendung eines Token möglich. Den berechtigten Mitarbeitern der Personalabteilung, der Führungskraft und den an einem Bewerbungsverfahren beteiligten Gremien ist es jedoch möglich, die Bewerberdokumente auch auszudrucken, um diese bei Vorstellungsgesprächen, welche an allen Standorten des rbb stattfinden können, vorliegen zu haben. Immerhin konnte ich aber erreichen, dass bei der Berechtigungsvergabe zu dem System ein deutlicher Hinweis zur Zweckbindung der Daten, zur Pflicht zum sorgsamen Umgang und zur Pflicht zur Datenvernichtung nach Abschluss des Bewerbungsverfahrens erfolgt. Voraussetzung der

Nutzung des Systems seitens der rbb-Mitarbeiterinnen und -Mitarbeiter ist der Nachweis einer Datenschutzschulung.

Seit 01.07.2017 befindet sich das System im Regelbetrieb. Verbesserungen bei Gebrauchstauglichkeit und Barrierefreiheit, welche auf den Erfahrungen der Nutzerinnen und Nutzer basieren, werden weiterhin mit dem Hersteller besprochen und nach Prüfung und im Rahmen der Möglichkeiten umgesetzt.

5. Einsatz von Videokameras zur Dokumentation von Baufortschritten

Im Berichtszeitraum entstand in mehreren Bereichen der Wunsch, über Bau- und Umbautätigkeiten in den rbb-Programmangeboten zu berichten und das auch mit Bild- und Videomaterial zu unterlegen. Beispiele sind die bildliche Dokumentation des Baus der Energiezentrale und der Umbau des Kulturradio-Studios.

Bei derartigen Videoaufzeichnungen sind auch Datenschutz- und Datensicherheitsaspekte zu berücksichtigen. Zusammen mit dem ISB habe ich daher eine Checkliste erarbeitet, die den Verantwortlichen eine Hilfestellung bieten soll, was in diesem Zusammenhang zu tun und zu beachten ist. Danach muss sichergestellt sein, dass die verwendete Technik und die Art und Weise der Datenverarbeitung keine Möglichkeit zum Missbrauch bieten. Wird eine Fremdfirma mit den Filmaufnahmen betraut, muss eine Vereinbarung über Auftragsdatenverarbeitung abgeschlossen werden. Vor Beginn der Bild-/Videoaufnahmen muss eine Einverständniserklärung der voraussichtlich betroffenen rbb-Mitarbeiterinnen und -Mitarbeiter sowie der Fremdfirmen eingeholt werden. Die Einverständniserklärung muss schriftlich erfolgen. In der Erklärung muss über den Verwendungszweck des Bildmaterials und die geplanten Verbreitungswege informiert werden. Auf die Freiwilligkeit der Einverständniserklärung ist explizit hinzuweisen (Personen, die nicht zu sehen seien wollen, müssen gepixelt bzw. herausgeschnitten werden).

An prominenter Stelle müssen Aushänge über die Bildaufnahmen, den Verwendungszweck und die geplanten Verbreitungswege informieren.

6. Gefährdungsbeurteilung psychischer Belastungen

Auf Wunsch der Intendantin hat der rbb eine Arbeitsgruppe gegründet, die sich damit beschäftigt, die bisherige Durchführung von Gefährdungsbeurteilungen zu überprüfen. Die Arbeitsgruppe unter der Leitung des Produktions- und Betriebsdirektors hat sich wiederholt getroffen und Möglichkeiten zur Durchführung von Gefährdungsbeurteilungen erarbeitet. Dabei lag der Fokus auf Online-Befragungen zu psychischen Belastungen in Ergänzung zu Gefährdungsbeurteilungen durch den Betriebsarzt und die Sicherheitsingenieure. In der Arbeitsgruppe wurde entschieden, zwei Gefährdungsbeurteilungen mit unterschiedlichen Anbietern als Piloten durchzuführen. Beide Firmen führen die Ermittlung psychischer Belastungen am Arbeitsplatz mit Unterstützung von Onlinebefragungen durch. Die erhobenen Daten werden auf externen Servern gespeichert, eine Speicherung auf internen Servern des rbb erfolgt nicht. Auch werden keine personenbezogenen Daten übermittelt und gesichert. Ich habe den Inhalt der Fragebögen geprüft und konnte mich im Übrigen davon überzeugen, dass die Befragungen vollumfänglich anonym erfolgen. Eine Rückführung auf einzelne Mitarbeiterinnen und Mitarbeiter ist demnach nicht möglich. Die Ergebnisse der Gefährdungsbeurteilung werden nur einem festgelegten Personenkreis zur Verfügung gestellt. Derzeit wird das Mitwirkungsverfahren mit dem Personalrat zu dem geplanten Verfahren durchgeführt. Vor Inbetriebnahme wird der rbb mit den Firmen Vereinbarungen zur Auftragsdatenverarbeitung abschließen.

7. Anonymes Hinweisgebersystems

Aus Anlass der auch im rbb geführten Debatte um #metoo plant die Intendanz gemeinsam mit der Frauenvertreterin und der Konfliktmanagerin die Einrichtung eines anonymen Hinweissystems über einen externen Server. Mitarbeiterinnen und Mitarbeiter, die über sexuelle Belästigung berichten bzw. kommunizieren möchten, können sich bisher persönlich u.a. an die Frauenvertreterin, die Konfliktmanagerin und an die Compliance-Beauftragte wenden. Zusätzlich soll nun ein niederschwelliges Angebot gemacht werden, anonym etwas zu melden bzw. in einen Dialog zu

treten. Geplant ist die Nutzung des BKMS-Systems, das über zahlreiche Zertifizierungen zu Datenschutz und Informationssicherheit verfügt. Den Wunsch der Intendantin, möglichst schnell eine solche zusätzliche Möglichkeit der Meldung zu schaffen, verstehe ich und möchte dem nicht im Weg stehen. Allerdings habe ich zusammen mit dem ISB angesichts der Sensibilität der Daten darauf gedrungen, vor Einführung des Systems zunächst alle Fragen zur Technik auf Seiten des rbb sowie alle dazugehörigen Prozesse zu klären. Der entsprechende Klärungsprozess dauert noch an.

8. Bring your own device

In meinem letzten Tätigkeitsbericht hatte ich erwähnt, dass vor allem im journalistischen Bereich bei vielen Mitarbeiterinnen und Mitarbeitern der Wunsch besteht, ihre privaten mobilen Geräte wie Tablets, Smartphones und Laptops auch dienstlich zu nutzen. Das hat für die Nutzer unter anderem den Vorteil, dass sie nicht parallel mit zwei mobilen Geräten gleichzeitig umgehen müssen – mit einem für dienstliche und einem anderen für private Zwecke. Nach wie vor gibt es leider kein umfassendes Konzept für den Einsatz privater Geräte im rbb. Die Schwierigkeit besteht nämlich darin, dass der rbb als im datenschutzrechtlichen Sinne verantwortliche Stelle auch dann für die ordnungsgemäße Verarbeitung von personenbezogenen Daten im Zusammenhang mit der dienstlichen Tätigkeit haftungsrechtlich verantwortlich ist, wenn die Datenverarbeitung auf privaten Geräten der Beschäftigten stattfindet. In der Konsequenz gibt es „Bring your own device“ (BYOD) nur mit den Einschränkungen, dass nur iOS-Geräte dafür infrage kommen und der Mitarbeiter/die Mitarbeiterin sich den rbb-Richtlinien unterwerfen muss. Das heißt, dass das iPhone oder iPad - auch wenn es privat gekauft ist – von den Mitarbeiterinnen und Mitarbeitern der OUI genauso behandelt wird wie ein dienstliches Gerät – mit allen Zugriffsmöglichkeiten bis hin zu dem Recht, Daten im Sicherheitsfall löschen zu dürfen. Daher ist es kein Wunder, dass bislang nur wenige Mitarbeiterinnen und Mitarbeiter unter diesen Bedingungen von BYOD Gebrauch gemacht haben.

9. Übermittlung von Vergütungsdaten an die Kommission zur Ermittlung des Finanzbedarfs

Im Herbst 2017 beabsichtigte die Kommission zur Ermittlung des Finanzbedarfs (KEF), ein Gutachten zum „Vergütungsniveau der öffentlich-rechtlichen Rundfunkanstalten" im Vergleich untereinander, mit dem öffentlichen Sektor und mit Dritten (kommerziellen Medienwirtschaft) zu erstellen und beauftragte mit der Erstellung die Beratungsgesellschaft Kienbaum Consultants International GmbH (Kienbaum). Im Speziellen sollten folgende Fragen beantwortet werden:

- In welchen Bereichen/Berufsgruppen ist das aktuelle Vergütungsniveau innerhalb der öffentlich-rechtlichen Rundfunkanstalten unterschiedlich?
- Wo ist es im Vergleich mit externen Dritten höher oder niedriger?
- Wie werden die festgestellten Abweichungen begründet?
- Welche Schlussfolgerungen können insbesondere hinsichtlich der Wirtschaftlichkeit aus dem Gutachten gezogen werden?

Die KEF hat die Rundfunkanstalten zu diesem Zweck mit der Übermittlung von anonymisierten Mitarbeiter-Daten gebeten. Ihre Anforderung hat sie auf die Regelungen zu den Aufgaben und Befugnissen der KEF gemäß §§ 2 ff. Rundfunkfinanzierungsstaatsvertrag (RFinStV) gestützt.

Der AK DSB hat die Anforderung der KEF geprüft und folgendes festgestellt:

Bei den angeforderten Datensätzen hätte bei einem Teil auf konkrete Personen geschlossen werden können. Es bestehen erhebliche Bedenken hinsichtlich der Frage, ob §§ 2 ff. RFinStV als Rechtsgrundlage für die Übermittlung der teilweise personenbeziehbaren und sensiblen Daten herangezogen werden können. Zweifelhaft ist insoweit eine hinreichend bestimmte datenschutzrechtliche Ermächtigungsgrundlage der KEF zur Verarbeitung personenbezogener Daten. Zur wirksamen Anonymisierung und dem Ausschluss des Personenbezugs der Daten bei Gruppen, die weniger als vier Personen zählen, hat der AK DSB daher die Bildung von Clustern emp-

fohlen. In den Fällen, in denen eine sinnvolle Zusammenfassung nicht möglich war und damit der Personenbezug nicht
wirksam ausgeschlossen werden konnte, war im Ausnahmefall die Einwilligung des Betroffenen in die Datenübermittlung erforderlich. Die Betroffen sollten auf die Freiwilligkeit der Einwilligung hingewiesen werden. Für diesen Fall hat der AK DSB auch darauf hingewiesen, dass eine Vereinbarung über eine Auftragsdatenverarbeitung zwischen der KEF und der von ihr betrauten Beratungsgesellschaft abgeschlossen werden musste.

Die Personalabteilung hat sich an diese Vorgaben gehalten und hat entsprechende Cluster gebildet. Auf die Übermittlung von personenbeziehbaren Daten konnte auf diese Weise verzichtet werden.

10. Zuverlässigkeitsüberprüfungen im Zusammenhang mit Akkreditierungen

Akkreditierungsverfahren werden seit vielen Jahren von Veranstaltern von politischen, gesellschaftlichen oder sportlichen Großveranstaltungen durchgeführt, um zu einem sicheren und reibungslosen Ablauf beizutragen. Dem Veranstalter obliegt es grundsätzlich, im Rahmen seines Hausrechts zu entscheiden, welchen Funktionsträgern (z. B. Caterer, Sicherheitspersonal, Journalisten) in definierten Bereichen der Zutritt ermöglicht werden soll. Je nach Gefährdungslage entscheidet der Veranstalter zusammen mit der zuständigen Polizeibehörde über die Frage, ob im Rahmen des Akkreditierungsverfahrens auch eine Zuverlässigkeitsüberprüfung erforderlich ist. Wird dies bejaht, unterstützt die Polizei den Veranstalter dahingehend, dass sie die vom Veranstalter bei den Akkreditierungsbewerbern abgefragten und der Polizei zur Verfügung gestellten personenbezogenen Daten mit polizeilichen ggf. auch nachrichtendienstlichen Informationssystemen abgleicht und ihn über das Ergebnis informiert. Die Mitteilung der Polizei ist eine Entscheidungshilfe für den Veranstalter, die Zulassung bzw. Ablehnung spricht dieser in eigener Verantwortung aus.

Für eine solche Sicherheitsüberprüfung benötigt die Polizei eine Rechtsgrundlage. Die Gesetzeslage und die tatsächliche Handhabung durch die Sicherheitsbehörden

sind in Bund und Ländern unterschiedlich. Im brandenburgischen Polizeigesetz gibt es z. B. bisher keine gesetzliche Ermächtigung für Zuverlässigkeitsüberprüfungen bei Großveranstaltungen. Einwilligungserklärungen der Betroffenen helfen hier nur bedingt weiter. Denn von Freiwilligkeit, die Voraussetzung einer rechtswirksam erteilten Einwilligung ist, kann z. B. bei Mitarbeitern der Rundfunkanstalten nur bedingt die Rede sein. Erteilt der/die Betroffene seine Einwilligung nicht, hat das mindestens zur Folge, dass er/sie einen bestimmten Dienst nicht übernehmen kann. Dennoch lässt sich der rbb immer wieder auf eine solche Praxis ein, da das grundsätzliche Anliegen (die Aufrechterhaltung der Sicherheit) ja ein nachvollziehbares Anliegen ist.

Im Vorfeld des Lollapalooza-Festivals 2017 in Hoppegarten haben sich Mitarbeiter an mich mit der Frage gewandt, ob sie tatsächlich verpflichtet seien, ihre persönlichen Daten an den Veranstalter herauszugeben und ihre Einwilligung in die Übermittlung der Daten an die Polizei zu erklären. Ich habe diese Anfrage zum Anlass genommen und mich an die Brandenburgische Landesdatenschutzbeauftragte gewandt. Die Behörde hat mir bestätigt, dass das vom Veranstalter gewählte Verfahren zwar grundsätzlich korrekt sei. Insbesondere hob sie die korrekte Datenschutzinformation zum Ablauf, Umfang, Beurteilungskriterien und Folgen der Zuverlässigkeitsüberprüfung hervor. Allerdings hat sie meine Skepsis hinsichtlich der Wirksamkeit der entsprechenden Einwilligungserklärungen geteilt. Sie hat dieses Verfahren zum Anlass genommen, mit dem zuständigen Ministerium Kontakt aufzunehmen, um die Rechtslage zu erörtern und für künftige Zuverlässigkeitsüberprüfungen einen rechtlich klarer abgesicherten Rahmen zu unterstützen.

Auf ihrer Sitzung am 09./10.11.2017 haben sich die Rundfunk-Datenschützer mit einer ähnlichen Problematik befasst: Die Deutsche Fußballliga GmbH (DFL) hat aufgrund der „höheren Sensibilität in sicherheitsrelevanten Fragen insbesondere bei Großveranstaltungen wie z. B. Fußballspielen“ dazu aufgefordert, dass alle zu akkreditierenden Personen, die mit der Produktion des Basissignals und der Erbringung von sonstigen technischen Leistungen oder als Hörfunk-Reporter tätig sind, ihren Vor- und Nachnamen, ihre private Anschrift, ihr Geburtsdatum sowie ihre Funktion in der Rundfunkanstalt an die DFL-GmbH übermitteln und diese dann die

Daten auch an die Fußballklubs weitergeben darf. Diese Forderung hat zu Recht zu Irritationen der Sportchefs von ARD, ZDF und DLR geführt. Denn im Unterschied zu vergleichbaren Akkreditierungsverfahren kam hier noch erschwerend hinzu, dass die Daten nicht anlassbezogen erhoben werden sollten, sondern quasi auf Vorrat. Die Rundfunkanstalten bzw. die Betroffenen hätten letztlich keine Kontrolle mehr darüber gehabt, wo genau die Daten für welche Zwecke wie lange gespeichert bleiben. Dies war inakzeptabel.

Im Ergebnis haben wir daher von einer entsprechenden Datenweitergabe unter diesen Voraussetzungen an die DFL abgeraten. Der Rundfunkdatenschutzbeauftragte des hr hat sich inzwischen auch an den zuständigen Hessischen Datenschutzbeauftragten gewandt. Die Behörde wird zunächst eine Stellungnahme der DFL einholen.

11. Veröffentlichung von Statistiken zum Frauenförderplan

Gemäß Frauenförderplan erstellt die Personalabteilung einmal jährlich Statistiken zum Frauenförderplan sowie eine Beschäftigtenstrukturanalyse. Bislang stellt die Personalabteilung diese Unterlagen lediglich der Frauenvertreterin, der Geschäftsleitung, dem Personalrat und der Senatsverwaltung für Frauen zur Verfügung. Im Intranet wird lediglich eine abgespeckte Form der Statistiken ohne absolute Zahlen veröffentlicht. Die Frauenvertreterin und die Personalchefin wünschen sich eine einheitliche Variante der Statistiken und der Beschäftigungsstrukturanalyse. Im Sommer 2017 hat sich deshalb eine Mitarbeiterin der Personalabteilung an mich mit der Frage gewandt, ob man nicht doch ggf. zu einer einheitlichen Variante kommen könnte.

Das Problem besteht darin, dass bei einigen Statistiken – insbesondere zu Vergütungsfragen – eine Personenbeziehbarkeit aufgrund der kleinen Anzahl von Personen, die zu einer Gruppe gehören (Cluster) nicht ausgeschlossen werden kann. Nach eingehender Prüfung musste ich der Personalabteilung daher mitteilen, dass auch zukünftig – mangels Vorliegen einer entsprechenden Rechtsgrundlage - die Veröffentlichung von personenbeziehbaren Daten im Rahmen der Statistiken zum Frauenförderplan im Intranet unterbleiben muss. Dafür spricht auch § 16 Abs. 5

des Landesgleichstellungsgesetzes (LGG), der die Pflicht der Frauenvertreterin zum Stillschweigen über persönliche Verhältnisse von Beschäftigten regelt. Damit hat der Gesetzgeber zum Ausdruck gebracht, welche Wichtigkeit der Geheimhaltung der personenbezogenen Daten und persönlichen Verhältnisse der Betroffenen im Rahmen des Frauenförderplans zuzumessen ist.

12. Datenschutzrechtliche Aspekte bei der Auslegung des Freienstatuts

In meinem letzten Tätigkeitsbericht habe ich über den Konflikt zwischen Personalabteilung und Freienvertretung hinsichtlich des der Freienvertretung zur Erfüllung ihrer Aufgaben regelmäßig zu übermittelnden Datenkatalogs der freien Mitarbeiterinnen und Mitarbeiter beim rbb berichtet (S. 40 ff.) Ich teile die Auffassung der Personalabteilung, dass den sehr weitgehenden Forderungen der Freienvertretung das Recht auf Datenschutz der Betroffenen entgegensteht. Nachdem hier keine Einigung erzielt werden konnte, hat die Freienvertretung am 06.04.2017 einen Antrag auf Einleitung eines Beschlussverfahrens vor dem Verwaltungsgericht Berlin gestellt. Sie beantragt festzustellen, dass der rbb verpflichtet ist, ihr über die ihr schon bislang regelmäßig zur Verfügung gestellten Daten umfangreiche Listen mit weiteren personenbezogenen Mitarbeiterdaten, wie z. B. Honorardaten, zur Verfügung zu stellen. Das VG Berlin hat noch keinen Verhandlungstermin in dieser Sache anberaumt (s. B III. 2.3).

13. #metoo

Die Intendantinnen und Intendanten der ARD haben auf ihrer Sitzung Anfang Februar 2018 in München die Juristische Kommission um eine Prüfung im Zusammenhang mit der #metoo- Debatte gebeten. Gegenwärtig laufen die Untersuchungen im Fall Wedel, ob sich in den Archiven der Rundfunkanstalten entsprechende Hinweise finden. Nicht auszuschließen ist, dass es daneben auch noch weitere Fälle gibt, die jetzt ans Tageslicht kommen. Konkret hat die Juristische Kommission den Auftrag zu prüfen, unter welchen Bedingungen Dritten Akteneinsicht bei Verdachtsfällen zu gewähren ist oder gewährt werden sollte. Die bisherige Sprachregelung lautet, dass

die Rundfunkanstalten anlassbezogenen in jedem Einzelfall prüfen werden, ob und wie Dritten Akteneinsicht gewährt werden kann. Dabei spielen der Datenschutz und die Persönlichkeitsrechte der Betroffenen eine maßgebliche Rolle für die erforderliche Güterabwägung.

14. E-Learning

Im Mai 2017 war im Intranet zu lesen, dass der rbb neuerdings ein eigenes E-Learning-Programm zur Erstellung kurzer sendefähiger Videos mit dem iPhone habe. Am Ende könne man sich sogar ein Teilnahmezertifikat ausdrucken. Entstanden war die Anwendung auf Initiative eines rbb-Mitarbeiters, jedoch ohne Absprache mit mir und dem Personalrat, obwohl datenschutz- und mitbestimmungsrechtliche Aspekte zu beachten waren.

Eine nachträgliche datenschutzrechtliche Überprüfung ergab, dass die Web-Anwendung von jedem PC im rbb per Webbrowser aus aufgerufen werden konnte, wenn dieser über einen Zugang zum rbb-Intranet verfügt. Die Webanwendung lag auf den Intranet-Ausspiel-Servern des rbb. Die Nutzung der Web-Anwendung sollte freiwillig und kostenlos sein. Um am Ende des Kurses ein Teilnahmezertifikat ausdrucken zu können, sollte zu Beginn der eigene Name in eine Maske eingetragen werden. Dieser sollte als Cookie auf dem PC abgelegt werden, an dem die E-Learning-Anwendung gestartet worden wäre. Sie hätte nur von der Person abgerufen werden können, die sich zum Start der Web-Anwendung eingeloggt hat. Damit waren die datenschutzrechtlichen Bedenken hinsichtlich des technischen Verfahrens zwar ausgeräumt. Der Personalrat hatte aber zu Recht die geplante Auswertung thematisiert, die eine Leistungskontrolle darstellte und in der Form mitbestimmungspflichtig war. Nach Änderung dieser Auswertung, die nun nur noch eine erfolgreiche Teilnahme attestiert, konnte der eLearning-Kurs wieder genutzt werden. Unklar war immer noch, ob die Vorlage einer Teilnahmebescheinigung Vorbedingung zur Ausleihe von Technik sein sollte.

V. Datenschutz in den Angeboten des rbb

1. Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten

Im September 2016 hat der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio Leitlinien zum Datenschutz in den öffentlich-rechtlichen Telemedien- und Social-Media-Angeboten verabschiedet (Anlage 2). Die Leitlinien konkretisieren die verbindlichen Vorgaben der Datenschutzgesetze und sollen den Verantwortlichen in den Rundfunkanstalten dabei helfen, datenschutzrelevante Themen zu erkennen und zu beurteilen. Sie bieten mit den Datenschutz-„Basics" einen Überblick über die wichtigsten datenschutzrechtlichen Grundprinzipien. Daneben liegt der Fokus auf praxisrelevanten Einzelthemen von A wie „Apps" bis W wie „Web-Analyse". Anhand von Checklisten wird dabei für jedes Thema umfassend dargestellt, worauf für eine datenschutzkonforme Realisierung zu achten ist. An der Erarbeitung der Leitlinien habe ich mitgewirkt. Sie müssen spätestens mit Inkrafttreten der ePrivacy-Verordnung überarbeitet werden.

2. Datenschutzregelungen im Lizenzvertrag der Rundfunkanstalten mit der AGF GmbH

Anfang 2017 wurde die bis dahin als Arbeitsgemeinschaft, bestehend aus den Landesrundfunkanstalten und deren Werbetöchtern sowie der ARD Sales & Services GmbH, dem ZDF, der RTL-Gruppe und der SAT.1/Pro7-Gruppe, bestehende „Arbeitsgemeinschaft Fernsehforschung" (AGF) in eine GmbH überführt, an der für die ARD als Treuhänder für alle übrigen Anstalten der hr und für die Werbetöchter der ARD-Landesrundfunkanstalten die ARD Sales & Services GmbH als Gesellschafter beteiligt sind. Mit der Reorganisation der AGF wurde außerdem das Forschungsfeld auf die Nutzungsmessung von Streaming-Diensten bei Nutzung stationärer PCs oder Notebooks wie auch bei Nutzung von mobilen Endgeräten wie z. B. Smartphones, Tablets, etc. ausgeweitet, wobei sich die AGF GmbH dabei des Dienstleisters „The Nielsen Company (Germany) GmbH" aus Hamburg bedient. Das dem vom hr

für alle Landesrundfunkanstalten und deren Werbetöchter mit der AGF abgeschlossenen Lizenzvertrag zugrunde liegende Geschäftsmodell sieht vor, dass Nielsen die Nutzungsdaten für jede Landesrundfunkanstalt im Wege der Auftragsdatenverarbeitung aufbereitet und in anonymisierter Form im Auftrag der Landesrundfunkanstalt der AGF für die Bewegtbildforschung zur Verfügung stellt. Die einzige datenschutzrelevante Übertragung personenbezogener Daten findet bei der Übermittlung der Nutzungsdaten zusammen mit der IP-Adresse der Nutzerinnen und Nutzer an das europäische Rechenzentrum von Nielsen in England statt. Dort werden die IP-Adressen – ohne Zwischenspeicherung – nach einem sog. Hash-Verfahren anonymisiert.

Die datenschutzrelevanten Regelungen im Lizenzvertrag mit der AGF und der Text der Mustervereinbarung über die Auftragsdatenverarbeitung, die jede Rundfunkanstalt mit Nielsen separat abschließen musste, wurde mit den Datenschutzbeauftragten von ARD und ZDF abgestimmt.

3. TVswift

Seit Anfang 2016 nutzt der rbb das Software-Produkt TVswift des deutschen Anbieters DAP GmbH. TVswift ist ein webbasiertes TV-Redaktionssystem, mit dem den Rundfunkanstalten die TV-Quoten der AGF täglich aufbereitet zur Verfügung gestellt werden. Der Zugriff erfolgt über eine verschlüsselte SSL-Verbindung und ist mit einem Benutzernamen und Passwort geschützt. Die Leiterin der Medienforschung Fernsehen des rbb hat die Administrationsrechte und pflegt eigenständig die Benutzer.

Dieser Nutzung liegt ein Rahmenvertrag zugrunde, den der NDR für alle ARD-Anstalten und deren Werbetöchter mit der DAP GmbH geschlossen hat. In diesem Rahmenvertrag gibt es auch einige Regelungen zu Datenschutz und Datensicherheit. Nachdem ich von dem Einsatz von TVswift beim rbb im Herbst 2016 erfahren habe, habe ich darauf gedrungen, dass der rbb zusätzlich zur Beitrittserklärung zum Rahmenvertrag noch eine Vereinbarung zur Auftragsdatenverarbeitung mit

der DAP GmbH abschließt, um den für ihn geltenden gesetzlichen Anforderungen zu genügen. Dies ist inzwischen geschehen.

Auf die ursprünglich vorgesehene Rückmeldung des Vertragspartners zum tatsächlichen Nutzungsverhalten der Mitarbeiterinnen und Mitarbeiter an die Administratorin wurde auf meine Intervention verzichtet.

4. RadioAnalyzer

Radioeins kam im Sommer 2017 auf den ISB und mich mit dem Wunsch zu, gemeinsam mit der Werbetochter des rbb, der rbb media, mithilfe der Software RadioAnalyzer die Programmnutzung der Hörer genauer zu analysieren, als es die normale Medienanalyse ermöglicht. Die Software funktioniert als sog. Software as a Service (SaaS). Sie ist web-basiert und läuft nur im Rechenzentrum des Herstellers in Dänemark. Analysiert wird das Hörerverhalten anhand des Angebots, das radioeins im Internet zur Verfügung stellt. Die Software liefert eine Analyse des Hörerverhaltens anhand von Log-Daten, die der Streaminganbieter von radioeins der Firma zur Verfügung stellt. Aus den Log-Daten werden anhand von IP-Adresse z. B. Einschaltzeitpunkt und Dauer des abgerufenen Audio-/Videostreams eines Hörers ermittelt und dann als Summe über alle Hörer dargestellt. In einem gemeinsamen Termin mit einem Vertreter des Herstellers, dem Leiter von radioeins, einem Mitarbeiter der rbb media, dem ISB und mir wurden Software und Auswertungsmöglichkeiten betrachtet. Zum Thema Datenschutz und Datensicherheit wurden folgende Punkte vereinbart:

- Die IP-Adressen der Hörer werden vor Übertragung der Log-Daten an die Firma per Hash anonymisiert.
- Das Anmeldeverhalten der radioeins-Mitarbeiter wird vom Anbieter – anders als ursprünglich vorgesehen – nicht protokolliert und ausgewertet.

Außerdem wurde mit dem Anbieter eine Vereinbarung zur Auftragsdatenverarbeitung abgeschlossen. Nachdem alle datenschutzrechtlichen Forderungen erfüllt waren, konnte ich dem Einsatz der Software zustimmen.

5. Neues Medienangebot von ARD und ZDF für Jugendliche und junge Erwachsene „funk“

Seit dem 01.10.2016 ist das Medienangebot von ARD und ZDF für Jugendliche und junge Erwachsene im Alter von 14 bis 29 Jahren funk online. Funk hat eine eigene Website (funk.net) und eine eigene App (funk-App). Der Schwerpunkt liegt allerdings auf der Verbreitung von Inhalten über Social Media-Plattformen wie YouTube, Facebook, Snapchat und Instagram.

ARD und ZDF sind ihrer in § 11 Abs. 5 Satz 3 RStV enthaltenen Pflicht, für die Verbreitung des Jungen Angebots auf Drittplattformen übereinstimmende Richtlinien, insbesondere zur Konkretisierung des Jugendmedienschutzes und des Datenschutzes, zu erlassen, nachgekommen. Diese Richtlinien zum Datenschutz sind diesem Bericht als Anlage 2 beigefügt. Der Datenschutzbeauftragte des SWR ist gemeinsam mit der Datenschutzbeauftragten des ZDF federführend für die Kontrolle der Einhaltung des Datenschutzes in der funk-Redaktion zuständig.

Vor der Bundestagswahl 2017 hat die funk-Redaktion des rbb mit dem Berliner Umfragedienstleister Civey GmbH zusammengearbeitet. Der Vorteil der Arbeitsweise dieses Unternehmens liegt darin, dass die Umfragen ausschließlich online durchgeführt werden und damit tatsächlich die Zielgruppe von funk, die kaum über ein Festnetztelefon verfügt und nur schwierig über Mobiltelefon für Umfragen zu erreichen ist, untersucht werden konnte.

An den Umfragen von Civey können nichtregistrierte und registrierte Personen teilnehmen. Üblicherweise wird ein kleines Programm, das sog. Widget, der Firma in die Website des Kunden eingebunden. In einem Gespräch mit Vertretern der Firma und dem Leiter der Funk-Redaktion des rbb wurde klar, dass die technische

Einbindung des Widgets in die funk-Seiten noch einige datenschutzrechtlichen Fragen aufgeworfen hat, die kurz vor der Bundeswahl nicht mehr zu lösen waren. So hatte ich mich u. a. dafür ausgesprochen, dass eine Vorschaltseite eingerichtet wird. Denn ohne diese Vorschaltseite wäre die IP-Adresse der Nutzer der funk-Seiten automatisch mit dem Aufruf der Seiten ohne Wissen und Wollen auch an Civey weitergeleitet worden. Für das Setzen der Cookies auch bei den nichtregistrierten Teilnehmern forderte ich mehr Transparenz ein.

Um mit der Zusammenarbeit starten zu können, hat funk zunächst darauf verzichtet, das Widget von Civey in die funk-Seiten einzubinden und hat von Civey unmittelbar statistische Daten bezogen. Dies ermöglichte die redaktionelle Arbeit mit den Daten noch vor der Bundestagswahl.

6. Verbreitung von Informationen von Inforadio per WhatsApp oder Telegram

Seit Mitte 2017 verbreitet Inforadio Informationen auch über die Messenger-Dienste WhatsApp oder Telegram. Interessenten erhalten von Inforadio zwei Mal täglich aktuelle Informationen aus Berlin & Brandenburg, Deutschland und der Welt direkt per WhatsApp oder Telegram auf ihr Smartphone geschickt. Inforadio arbeitet dafür mit dem Online-Tool „WhatsATool“ von der österreichischen Firma atms. Die Nachrichten werden über das Online-Tool versendet. Bei Newslettern per WhatsApp und Telegram handelt es sich, genauso wie bei einem E-Mail-Newsletter, um elektronische Post, die nur mit Zustimmung des Empfängers versandt werden darf. Deshalb muss sich der Nutzer selbst registrieren, um das neue Angebot zu erhalten. Eine Abmeldung vom Dienst ist jederzeit möglich. Auf diesen Widerruf weist der rbb in der Datenschutzerklärung ausdrücklich hin. Die Daten der Nutzer werden auf Servern in Österreich gespeichert. Zu diesen Daten zählen alle SIM-Karten und alle Handynummern der registrierten Kontakte. Der rbb hat mit atms eine Vereinbarung über Auftragsdatenverarbeitung abgeschlossen.

Wie in meinen früheren Berichten ausgeführt, sehe ich die Verbreitung der rbb-Angebote über Facebook, Twitter und WhatsApp kritisch. Dies habe ich auch wiederholt gegenüber meinen Programmkollegen zum Ausdruck gebracht. Von den Kollegen wird mir dann immer entgegengehalten, dass der rbb die Nutzer lediglich dort abholt, wo sie sich ohnehin schon befinden. Immerhin werden die Informationen nicht exklusiv über diese Drittanbieter verteilt, sondern sind auch auf der Homepage von Inforadio abrufbar. Der Nutzer muss also die Drittplattformen nicht nutzen, um an die Informationen heranzukommen.

7. Archivierung von Tweets und Kommentaren im rbb-Archiv

2017 wurde im rbb mit meiner Zustimmung ein selbstgebautes Social Media-Recherche-Tool eingeführt, mit dem Journalisten zu einzelnen Themen Tweets und Facebook-Kommentare recherchieren können. Bei der Einführung war ich vorsichtig und hatte votiert, dass die Veröffentlichungen nur so lange im rbb vorgehalten werden, wie die Tweets und Kommentare selbst noch abrufbar sind. Das war zunächst auch deshalb kein Problem, weil mit entsprechenden Links gearbeitet wurde. Nachdem die journalistischen Kollegen einige Erfahrung gesammelt hatten, kristallisierte sich der Wunsch heraus, auch gelöschte Tweets und Kommentare noch für einige Zeit zu Recherchezwecken im Archiv vorzuhalten. Ich habe auch dazu meine Zustimmung erteilt. Die Archivierung ist vom Medienprivileg gedeckt. Dafür, dass sich die Nutzer von Facebook und Twitter Medien gegenüber nicht auf das Recht auf Vergessen berufen können, sprechen beispielsweise auch entsprechende Passagen in den Allgemeinen Geschäftsbedingungen der Plattformen. Ich habe darauf hingewiesen, dass die Journalisten bei der Nutzung und Veröffentlichung von inzwischen gelöschten Äußerungen auf diesen Umstand hinweisen müssen.

8. LU-Smart-App

Die LU-Smart-App ergänzt die Produktionsmittel im rbb um eine weitere Möglichkeit, Video- und Audiodaten mit mobilen Geräten direkt über das Mobilfunknetz und/oder eine WLAN-Verbindung an den rbb zu übertragen, um dann live über den

Fernsehschaltraum in Berlin ins Fernsehprogramm oder in ein Onlineangebot des rbb geschaltet zu werden. Die App ist sehr wichtig für die aktuelle Berichterstattung und auch für ARD-Aktuell, weil die Programmkollegen damit bei einem unvorhergesehenen Ereignis die Möglichkeit haben, Video- und Audiodaten sehr schnell ins Programm zu bringen. Die App läuft auf modernen Smartphones und Tablets mit den Betriebssystemen iOS oder Android. Allerdings ist es mit der App alleine nicht möglich, Daten an den rbb zu übertragen. Dazu muss man sich außerdem noch von den Mitarbeitern des Fernsehschaltraums als Nutzer registrieren lassen.

Der LU-Smart-Reporter vor Ort benutzt dabei das Smartphone, bis die professionelle Broadcasttechnik vor Ort ist. Außerdem kann man mit der LU-Smart-App grundsätzlich auch zuvor aufgenommene Videoclips in den rbb senden, dies nennt man „Store & Forward". Bislang war nicht gewährleistet, dass die Clips ausschließlich über europäische Server laufen, da der Datenverkehr über Cloud-Lösungen des Herstellers geführt wird. Das war für die Live-Berichterstattung gerade noch so hinnehmbar, da diese Daten ja damit ohnehin öffentlich sind. Etwas anderes gilt für die vorproduzierten Videoclips, die aus rechtlichen Gründen (z. B. zur Wahrung der Persönlichkeitsrechte der abgebildeten Protagonisten) vor Ausstrahlung ggf. noch bearbeitet werden müssen. Auf meine Initiative haben mehrere ARD-Anstalten und das ZDF, die diese Technik schon nutzen, an einer Lösung gearbeitet, bei der sämtlicher Datenverkehr über den ARD-Sternpunkt geführt wird. Seit dem 15.01.2018 läuft der Datenverkehr jetzt komplett über den ARD-Sternpunkt. Zuvor war beim rbb die „Store & Forward"-Lösung nicht im Einsatz.

9. Vereinbarkeit von Medienprivileg und Recherche-Zugriffen für Verwertungstöchter und Auftragsproduzenten

Auf seiner Sitzung am 03./04.11.2016 beim SR in Saarbrücken hat der AK DSB folgenden Beschluss gefasst:

Ein Recherchezugriff der Verwertungstöchter der Rundfunkanstalten auf die Archivbestände (Fernsehen, Hörfunk) der gesamten ARD (Cross-Recherche) verstößt nicht gegen das Medienprivileg. Voraussetzung ist, dass die gewonnenen Daten im

Rahmen einer Publikation verarbeitet und nicht für individuelle Anfragen beliebiger Interessenten verwendet werden. Der AK DSB hat ausdrücklich auf den Ausschließlichkeitscharakter der publizistischen Zweckbestimmung verwiesen.

Auf dieser Grundlage hat der rbb der rbb media einen entsprechenden Recherchezugriff eingeräumt.

VI. Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung

1. Allgemeines

Für den Einzug der Rundfunkbeiträge betreiben die Landesrundfunkanstalten auf der Grundlage von § 10 Abs. 7 Rundfunkbeitragsstaatsvertrag (RBStV) im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft den Zentralen Beitragsservice „ARD ZDF Deutschlandradio Beitragsservice" (ZBS) in Köln. Soweit der ZBS für den rbb tätig wird, gelten die bereichsspezifischen Datenschutzregelungen des RBStV und ergänzend die Regelungen des BlnDSG.

Die Überwachung des Datenschutzes bei der Verarbeitung der Rundfunkteilnehmerdaten obliegt der Beauftragten für den Datenschutz des Landes Berlin im Benehmen mit der Landesbeauftragten für den Datenschutz des Landes Brandenburg (§ 38 Abs. 8 rbb-StV). Als behördliche Datenschutzbeauftragte gemäß § 19 a BlnDSG bin ich für die ordnungsgemäße Datenverarbeitung beim rbb und beim ZBS unmittelbar zuständig.

Unbeschadet der Zuständigkeit des nach Landesrecht für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ist beim ZBS gemäß § 11 Abs. 2 Satz 1 RBStV ein/e behördliche/r Datenschutzbeauftragte/r des Beitragsservice zu bestellen. Die/der behördliche Datenschutzbeauftragte arbeitet zur Gewährleistung des Datenschutzes mit dem/der nach Landesrecht für die jeweilige Rundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese/n über Verstöße gegen Datenschutzvorschriften sowie über die dagegen getroffenen

Maßnahmen. Im Übrigen gelten die für die/den behördlichen Datenschutzbeauftragten anwendbaren Bestimmungen des BDSG entsprechend. Die behördliche Datenschutzbeauftragte übt diese Aufgabe neben ihrer Tätigkeit als Abteilungsleiterin beim ZBS aus. Seit 01.06.2006 wird sie durch eine Vollzeitkraft bei der Wahrnehmung ihrer Datenschutzaufgaben unterstützt.

Die Datenschutzbeauftragte und ihr Mitarbeiter leisten seit Jahren sehr professionelle und kompetente Arbeit. Es ist im Wesentlichen ihr Verdienst, dass der ZBS aus datenschutzrechtlicher Sicht sehr gut aufgestellt ist und das Vertrauen der Bevölkerung genießt.

2. Auskunftsersuchen und Eingaben

Die Datenschutzbeauftragten der Rundfunkanstalten haben die Bearbeitung und Beantwortung von Anfragen und sonstigem Routineschriftwechsel in Datenschutzangelegenheiten dem ZBS übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung haben sie sich selbst vorbehalten.

Im Jahr 2017 hat die Datenschutzbeauftragte des ZBS folgende Vorgänge aus dem Sendegebiet des rbb für mich bearbeitet:

Ersuchen von Bürgerinnen und Bürgern um Auskunft über zu ihrer Person gespeicherter Daten:	50 (Vorjahr 49)
Fragen bezüglich der Herkunft von Daten (z. B. Adressen) bzw. der Berechtigung zur Datenerhebung:	12 (Vorjahr 5)
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen:	8 (Vorjahr 41)

Anfragen von Finanzämtern nach Daten (insbesondere Bankverbindungen) von Beitragszahlerinnen und –zahlern:	0 (Vorjahr 0)
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Beitragszahler(n)/innen	2 (Vorjahr 0)
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	7 (Vorjahr 11)
Anzahl der Vorgänge insgesamt:	**79 (Vorjahr 106**)

Ich selbst habe in 2017 folgende Vorgänge bearbeitet:

Ersuchen von Bürgerinnen und Bürgern um Auskunft über zu ihrer Person gespeicherter Daten:	10 (Vorjahr 8)
Fragen bezüglich der Herkunft von Daten (z. B. Adressen) bzw. der Berechtigung zur Datenerhebung:	0 (Vorjahr 0)
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen:	0 (Vorjahr 2)
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz:	5 (Vorjahr 2)
Anzahl der Vorgänge insgesamt:	**15 (Vorjahr 12)**

Ein Teil der Auskunftsersuchen und Eingaben erreicht die Datenschutzbeauftragte des ZBS bzw. mich direkt, ein anderer Teil erreichte mich über die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

In 2017 waren zwei Eingaben erfolgreich:
Es wurde moniert, dass bei Briefsendungen des ZBS die unverschlüsselte Beitragsnummer im Adressfeld der Schreiben abgedruckt war. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit sah darin ein personenbezogenes Merkmal, dessen Verarbeitung eine Rechtsgrundlage erfordert. Zwar dürften personenbezogene Daten im Zusammenhang mit dem Beitragseinzug auch ohne Einwilligung der Betroffenen verarbeitet werden, jedoch nur dann, wenn und soweit dies für die Verwaltungstätigkeit erforderlich ist. In früheren Jahren hatten die Rundfunkanstalten angeführt, dass die Sichtbarkeit der Beitragsnummer im Adressfenster zur schnelleren und wirtschaftlichen Abwicklung des Rundfunkeinzugs erforderlich ist. Über die im Adressfeld sichtbare Beitragsnummer und die zusätzliche Vordrucknummer wurden die unzustellbar zurückkommenden Sendungen ohne Öffnung der Briefhülle und Entnahme des Inhalts verarbeitet. Mittlerweile gibt es aber durch eine neue Technik die Möglichkeit, die Beitragsnummer verschlüsselt im OCR-Code zu hinterlegen. Der ZBS hat daher zugesichert, auf diese neue Technik umzusteigen.

Mit einer weiteren Eingabe wurde kritisiert, dass der ZBS für den rbb im Rahmen eines Vollstreckungsersuchens an eine Vollstreckungsbehörde neben der Angabe der rückständigen Beiträge auch die Tatsache aufgeführt hat, dass der Schuldner aktuell von der Rundfunkbeitragspflicht befreit sei. Dieses Verfahren entsprach zum damaligen Zeitpunkt der Üblichkeit. Da ich für die Übermittlung dieses Datums keine Rechtsgrundlage gesehen habe und überdies die Mitteilung über einen Befreiungsstatus für die Arbeit der Vollstreckungsbehörden auch nicht erforderlich war, habe ich angeregt, auf die Mitteilung dieses Datums zukünftig zu verzichten. Nach Diskussion innerhalb der zuständigen Gremien innerhalb der ARD wurde dieses so umgesetzt.

3. Projekt EUDAGO

Schon im Juni 2017 hat der Zentrale Beitragsservice (ZBS) ein aufwändiges und kostenintensives Projekt unter dem Titel „EUDAGO“ (Umsetzung der Anforderun-

gen aus der EU-Datenschutzgrundverordnung) zur Implementierung eines DSGVO-konformen Datenschutzmanagementsystems beim ZBS gestartet. Nach den mir vom Verwaltungsdirektor zur Verfügung gestellten Unterlagen sind die Arbeiten dort offenbar schon sehr weit fortgeschritten. Die notwendigen Anpassungen von Prozessen und Verfahren des Beitragseinzugs sowie für eine Vielzahl von Verträgen im Beschaffungsbereich sollen laut Plan bis Ende Mai 2018 vollständig abgeschlossen sein. Leider sind die Datenschutzbeauftragten der Rundfunkanstalten in das Projekt nur sehr lose eingebunden gewesen. Durch diesen Alleingang wurde die Chance auf Synergieeffekte für die Rundfunkanstalten vertan.

4. Vorbereitungen für den weiteren Meldedatenabgleich

Zum Stichtag 06.05.2018 wird nach § 14 Abs. 9a RBStV ein weiterer, vollständiger Abgleich der Meldedaten durchgeführt. Im Berichtszeitraum lag beim ZBS ein Themenschwerpunkt auf den erforderlichen Vorbereitungen dazu. Schon 2013 fand ein solcher Abgleich erstmalig statt. Wie in meinem letzten Tätigkeitsbericht ausgeführt, hat der 19. RÄndStV die Möglichkeit zu einem weiteren vollständigen Meldedatenabgleich eröffnet. Dafür ist die Befugnis zum Adressankauf bis zum 31.12.2020 weiter ausgesetzt worden. Im Vorfeld hatte der AK DSB die Einräumung einer solchen Möglichkeit befürwortet. Aus seiner Sicht haben die Rundfunkanstalten überzeugend dargelegt, dass allein die staatsvertraglichen Anzeigepflichten und Auskunftsrechte nicht ausreichen, um einer erneuten Erosion des Teilnehmerdatenbestandes wirksam vorzubeugen. Die Durchführung eines erneuten Meldedatenabgleichs ist nach unserer Überzeugung das mildeste und am besten geeignete Mittel, diesen Entwicklungen vorzubeugen – dies vor dem Hintergrund der strikten Zweckbindung und der in der Praxis problemlosen und von wenig Beschwerden begleiteten reibungslosen Durchführung des Meldedatenabgleichs im Jahr 2013.

Folgendes Vorgehen ist vorgesehen:

Zum Stichtag 06.05.2018 werden die Meldedaten aller volljährigen Personen durch die Einwohnermeldeämter gesichert. Ab dem 07.05.2018 findet sodann die

Übermittlung der Meldedaten gemäß einem abgestimmten Lieferkonzept an den ZBS statt. Der ZBS nimmt dann eine Prüfung der Daten vor, indem er diese zunächst nach bekannten und unbekannten Personen aufteilt. Alle Meldedaten zu bekannten Personen werden unmittelbar gelöscht. Nicht bekannte Personen erhalten bis zu zwei Klärungsbriefe mit der Bitte um Klärung der Sachlage (Ausbringung Juni 2018 bis Mai 2019). Bei Rückmeldung, dass bereits für die entsprechende Wohnung ein Beitrag gezahlt wird, erfolgt der Abschluss der Klärung und die Daten zu der Person werden gelöscht. Bei Rückmeldung, dass für die entsprechende Wohnung noch kein Beitrag gezahlt wird, erfolgt eine Anmeldung der Person. Erfolgt keine Rückmeldung auf die Klärungsschreiben, wird die Person aufgrund der gesetzlichen Vermutung gemäß § 2 Abs. 2 Satz 2 Ziffer 1 RBStV („Als Inhaber einer Wohnung wird jede Person vermutet, die dort nach dem Melderecht gemeldet ist…") angemeldet.

Die Rechtmäßigkeit des Meldedatenabgleichs wurde anlässlich des erstmaligen Abgleichs im Jahr 2013 von mehreren Obergerichten – unter anderem dem OVG Berlin-Brandenburg (Entscheidung vom 06.08.2013) festgestellt.

5. Überarbeitung Historielöschkonzept

Vor dem Hintergrund der verschärften Gesetzesforderung nach Datenminimierung durch die DSGVO hat der ZBS endlich die von den Rundfunk-Datenschützern bereits seit einigen Jahren geforderte Überarbeitung des Historielöschkonzepts begonnen. Das seinerzeit mit dem AK DSB abgestimmte Historielöschkonzept ist seit März 2007 in Kraft. In Vorbereitung der Überarbeitung dieses Konzepts hat der ZBS zunächst externe Expertise zur Klärung der Aufbewahrungsfristen in Anspruch genommen. Aus datenschutzrechtlicher Sicht sind Daten grundsätzlich nur solange zu speichern, wie sie zur Erfüllung des Beitragseinzugs erforderlich sind. Andererseits bestehen nach den Regelungen des Handelsgesetzbuchs (HGB) Aufbewahrungspflichten, die einer Löschung entgegenstehen können. Angesichts der Komplexität wurde ein zweistufiges Vorgehen beschlossen. Bis Ostern 2018 werden zunächst alle nicht mehr benötigten Daten aus der alten Rundfunkgebührenwelt (bis 2012)

gelöscht. Der ZBS hat angekündigt, dem AK DSB im Frühjahr 2018 einen Vorschlag für die zweite Löschstufe zu unterbreiten.

D. Datenschutz im Informationsverarbeitungszentrum (IVZ)

1. Allgemeines

Beim rbb wird als Gemeinschaftseinrichtung das rechtlich unselbstständige Informationsverarbeitungszentrum (IVZ) betrieben. Seit einiger Zeit gibt es eine große Zweigstelle beim WDR. Rückwirkend zum 01.01.2017 sind der BR, der hr und der SWR dem IVZ beigetreten, so dass das IVZ inzwischen von allen ARD-Anstalten und dem DLR gemeinsam getragen wird. Wegen des Beitritts der Rundfunkanstalten ist die Verwaltungsvereinbarung des IVZ geändert worden. Bei dieser Gelegenheit wurden auch die Regelungen zu Datenschutz und Informationssicherheit in der Verwaltungsvereinbarung klarer gefasst. Für die Kontrolle des Datenschutzes und der Datensicherheit sind alle Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Als Datenschutzbeauftragte der Sitzanstalt bin ich federführend zuständig.

Nachdem die langjährige und sehr erfahrene ISB des IVZ Frau Christiane Fackeldey ihr Amt niedergelegt hat, ist zum 01.02.2017 Herr Dieter Paustian vom Geschäftsführer des IVZ zum neuen ISB bestellt worden. Herr Paustian nimmt diese Aufgabe im Wesentlichen von seinem Homeoffice in Kiel wahr. Aus meiner Sicht sollte ein ISB in einem Unternehmen, deren Geschäftszweck die elektronische Datenverarbeitung ist, für den Fall etwaiger Sicherheitsvorkommnisse stets vor Ort ansprechbar sein. Da es an beiden Standorten des IVZ – in Köln und Berlin – einen stellvertretenden ISB gibt, ist die überwiegende Abwesenheit des ISB aber akzeptabel. Zusätzlich wird zukünftig die RBT das IVZ im Bereich Informationssicherheit beraten.

2. Einbeziehung der Rundfunkdatenschutzbeauftragten

Am 12.12.2016 fand das Jahrestreffen zu Datenschutz und Informationssicherheit im IVZ statt. Aus datenschutzrechtlicher Sicht waren der Bericht zum BSI-Rezertifizierungsaudit 2016, die Präsentation des geplanten Wechsels vom IT-Grundschutz auf die internationale ISO-Norm 27001 und der Bericht über die Sicherheitsvorfälle in 2016 von besonderem Interesse.

Auf ihrer Sitzung am 30./31.03.2017 beim NDR haben sich die Rundfunk-Datenschutzbeauftragten mit dem Thema „Datenschutz beim IVZ" befasst. Unter anderem wurde kritisiert, dass die Rundfunkdatenschutzbeauftragten in letzter Zeit nicht mehr – wie in der Verwaltungsvereinbarung geregelt – unverzüglich über Sicherheitsvorfälle mit datenschutzrechtlicher Relevanz informiert werden. Auf Vermittlung des IVZ-Verwaltungsrats habe ich mit dem Geschäftsführer des IVZ inzwischen eine Reihe von Verabredungen zur zukünftigen Zusammenarbeit mit den Rundfunkdatenschutzbeauftragten vereinbart, die auf dem IVZ-Jahrestreffen am 12.10.2017 von den anderen Rundfunk-Datenschutzbeauftragten bestätigt wurden. Ein weiteres wichtiges Thema auf dem Jahrestreffen war die Nutzung des Microsoft-Produkts Office 365. Das IVZ nutzt MS Office 365 nur für eine übersichtliche Lizensierung. Installationen und Speicherorte der Daten befinden sich im IVZ. Es werden keine Cloud-Dienste verwendet. Außerdem wurde über die IVZ Reorganisation und die aktuellen Projekte im IVZ gesprochen.

3. ARD-ZDF-Vote

Die vor einigen Jahren eingeführte Eigenentwicklung „ARD-ZDF-Vote" des IVZ dient dem Erstellen von Terminabstimmungen und Umfragen. Sie wird am Standort Berlin des IVZ für die ARD, das ZDF und Deutschlandradio betrieben und ist eine sichere Alternative zu dem aus datenschutzrechtlicher Sicht nicht empfehlenswerten Tool eines Schweizer Anbieters Doodle. Die Kritik an Doodle besteht insbesondere an einem mangelnden Zugriffsschutz. Die Entwicklung und Wartung von ARD-ZDF-Vote obliegen dem IVZ. Die Daten bleiben intern. Im Sommer 2017 hat das IVZ

dieses Tool aktualisiert und technisch und gestalterisch angepasst. Zugleich wurde der Dienst nun auch – mit eingeschränktem Funktionsumfang - über das Internet zugänglich gemacht. Damit kann nun auch externes Personal bei Terminfindungen und Abstimmungen mit eingebunden werden und der Einsatz von Doodle ist gänzlich verzichtbar. Auf der Basis eines vom IVZ vorgelegten IT-Sicherheitskonzepts konnten die Rundfunkdatenschutzbeauftragten dem Einsatz des überarbeiteten Tools zustimmen.

4. Neue technische Plattform für das Helpdesk-System „IVZRequest"

Das IVZ beabsichtigt, die technische Plattform von „IVZ-Request" von einer Eigenentwicklung zu der von der gesamten ARD zukünftig genutzten Technik OTRS umzustellen. Seit Herbst 2017 findet mit meiner Zustimmung ein Probebetrieb des neuen Systems im IVZ statt, an dem ausschließlich Mitarbeiterinnen und Mitarbeiter des IVZ teilnehmen. Alle Mitarbeiterinnen und Mitarbeiter des IVZ haben rbb-Arbeitsverträge, so dass neben dem rbb-Personalrat und der rbb-Datenschutzbeauftragten keine Gremien der anderen Landesrundfunkanstalten einbezogen werden mussten. Während des Probebetriebs soll durch die Projektgruppe der Übergang vom aktuellen IVZ-Request zum OTRS erarbeitet werden. Das OTRS-System soll auf die etablierten Prozesse angepasst und die möglichen Veränderungen in den Prozessen herausgearbeitet werden. Auf diese Weise werden Abweichungen zur bislang gültigen Dienstvereinbarung zum IVZ erkannt. Künftig soll es einen ARD-weiten Helpdesk – basierend auf OTRS – geben. Der OTRS-Probebetrieb ist der erste Schritt des IVZ hin zur Teilnahme am zentralen Helpdesk.

E. Datenschutz beim ARD-Hauptstadtstudio

Das ARD-Hauptstadtstudio (HSB) ist ebenfalls eine rechtlich unselbstständige Gemeinschaftseinrichtung der ARD, für das der rbb als Sitzanstalt Federführer ist. Damit bin ich auch als Datenschutzbeauftragte federführend für diese Einrichtung zuständig. Alle rbb-Regelwerke zu Datenschutz und Informationssicherheit werden

im HSB entsprechend angewandt. Der Informationsfluss ist durch die beratende Mitgliedschaft des Bereichsleiters Systemservice des HSB im rbb-IST gewährleistet.

Seit Sommer 2016 bin ich mit den Verantwortlichen im HSB zu den Anforderungen an korrekte Datenschutzhinweise für die HSB-Website und den HSB-Blog im Gespräch. Beide Angebote sind technisch und organisatorisch voneinander getrennt. Während für die HSB-Website nun alle Fragen geklärt und die Datenschutzhinweise angepasst sind, sind für den HSB-Blog nach wie vor einige Fragen offen.

F. Informationsmaßnahmen

Am 02.05., 20.06. und 22.11.2016 sowie 28.04., 11.07. und 26.09.2017 habe ich gemeinsam mit dem ISB die für Führungskräfte des rbb obligatorische Schulung zu Datenschutz und Informationssicherheit durchgeführt.

Am 22.08.2016 und 01.09.2017 habe ich gemeinsam mit dem ISB die neuen Auszubildenden des rbb für Datenschutz und Informationssicherheit sensibilisiert. Mein Stellvertreter Axel Kauffmann hat gemeinsam mit einer Kollegin der OUI im Berichtszeitraum an folgenden Tagen die für SAP-Nutzer obligatorische Datenschutzschulung durchgeführt: 05.04., 07.06., 21.09., 12.10. und 07.12.2016, 04.01., 14.02., 04.04., 06.06., 24.08., 10.10. und 12.12.2017 sowie 13.02.2018.

An folgenden Tagen habe ich bzw. hat Herr Kauffmann gemeinsam mit dem ISB für die Teilnehmerinnen und Teilnehmer am Probebetrieb von MS Office 365 Schulungen zu Datenschutz und Datensicherheit durchgeführt: 19., 23. und 24.10. sowie 30.11.2017 (Herr Kauffmann).

Wie in meinen früheren Berichten ausgeführt, halte ich E-Learning-Angebote aber grundsätzlich für eine gute Möglichkeit, Mitarbeiterinnen und Mitarbeitern Inhalte zusätzlich zu Präsenzschulungen zu vermitteln. Auch für eine erste Einführung in die Themen Datenschutz und Datensicherheit wäre so ein Angebot nützlich.

Am 08.05.2017 habe ich mich gemeinsam mit dem ISB beim MDR über das dortige E-Learning-Angebot informiert. Das ansprechende Angebot des MDR basiert auf einem Standardprodukt eines Berliner Herstellers.

Im November 2017 hat der Hersteller für den Leiter der Abteilung Personalstrategie und Entwicklung, den ISB und mich eine Präsentation seines Angebotes in den Räumlichkeiten des rbb durchgeführt. Die Firma bietet selbst interessante Inhalte zum Datenschutz an, die unternehmensspezifisch angepasst werden können. Vor dem Hintergrund, dass der Transformationsprozess für die DSGVO im rbb noch nicht abgeschlossen ist, haben wir dieses Thema noch einmal zurückgestellt und werden darauf zurückkommen, wenn die Ergebnisse des Projekts zur Transformation der DSGVO (s. C II. 1.) vorliegen.

G. Sonstiges

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten arbeiten im Arbeitskreis der Datenschutzbeauftragten (AK DSB) zusammen. Ein wesentliches Ziel ist es dabei, den Datenschutz bei den gemeinsamen Programmangeboten und beim Beitragseinzug nach möglichst einheitlichen Kriterien – d. h. in der Praxis, nach den jeweils höchsten Anforderungen – sicherzustellen.

Im Berichtszeitraum fanden Sitzungen am 14./15.04. in Berlin (rbb) und 3./4.11.2016 in Saarbrücken (SR) sowie am 30./31.03.2017 in Hamburg (NDR) und am 09./10.11.2017 in Berlin (DLR) statt.

Auf unseren Sitzungen haben wir unter anderem folgende Themen erörtert:

- Fragen im Zusammenhang mit der Transformation der DSGVO
- Einzelfragen zur Rundfunkteilnehmerdatenverarbeitung

- Möglichkeiten der Verbesserung der IT-Sicherheit
- Cloud Computing
- Nutzung von Microsoft Office 365
- Bildberichterstattung/Minderjährigen-Datenschutz

Zum Vorsitzenden des AK DSB für die Jahre 2017 und 2018 wurde Herr Stephan Schwarze (MDR) gewählt. Ich wurde für den gleichen Zeitraum zur Stellvertreterin gewählt.

II. Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern

Im Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern werden aktuelle und strategische Fragen des Datenschutzes aus den Bereichen Telekommunikations-, Multimedia- und Rundfunkrecht erörtert. Viele Jahre hatte der Berliner Datenschutzbeauftragte den Vorsitz des AK Medien inne. Seit Anfang 2017 teilen sich die Landesdatenschutzbeauftragte von Berlin, Frau Smoltczyk, und der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Herr Kranig, den Vorsitz. In der Vergangenheit hatte regelmäßig ein Mitglied des AK DSB an einem Teil der Sitzung des AK Medien teilgenommen. Auf der Sitzung am 01./02.03.2016 hat die Datenschutzbeauftragte des SR, Sonnia Wüst, den AK DSB vertreten.

Anfang 2017 hat der AK DSB beschlossen, nicht mehr regelmäßig an den Sitzungen des AK Medien teilzunehmen. Aus seiner Sicht sind regelmäßige Treffen in einer kleineren Gruppe von Vertreterinnen und Vertretern beider Arbeitskreise, um den Kontakt zu intensivieren, sinnvoller. Einen entsprechenden Vorschlag hat der AK Medien angenommen. In diesem Sinne fand am 31.01.2017 beim HR in Frankfurt ein erster Gedankenaustausch zwischen staatlichen Datenschutzbeauftragten und Rundfunkdatenschutzbeauftragten statt. Themen waren der Minderjährigen-Datenschutz, die Einhaltung des Datenschutzes beim Beitragsservice, die Umsetzung der DSGVO und der Einsatz von Cloud-Technologien. Das Treffen verlief sehr angenehm und konstruktiv.

III. Zusammenarbeit der datenschutzrechtlichen Aufsichtsbehörden nach der DSGVO

Nach dem DSAnpUG-EU fällt der Bundesdatenschutzbeauftragten die Aufgabe zu, auf die Zusammenarbeit der öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, hinzuwirken (§ 16 Abs. 5 DSAnpUG-EU). In § 18 Abs. 1 DSAnpUG-EU ist zudem festgehalten, dass die Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union die nach Art. 85 und 91 DSGVO eingerichteten spezifischen Aufsichtsbehörden beteiligen, sofern diese von der Angelegenheit betroffen sind.

Am 29.09.2017 fand auf Einladung der Bundesdatenschutzbeauftragten Andrea Voßhoff ein erstes Treffen statt. An dem Termin nahmen neben Frau Voßhoff und ihren Mitarbeitern Vertreter der staatliche Aufsichtsbehörden, Vertreter der Kirchen, des Presserats und des DJV sowie einige Vertreter des AK DSB teil. Die Vertreter des AK DSB machten deutlich, dass wir ein hohes Interesse an einer Abstimmung mit den anderen nationalen Aufsichtsbehörden haben. Dabei interessiert uns Rundfunkdatenschutzbeauftragten nicht nur eine Abstimmung in Medienfragen, sondern insbesondere auch in anderen datenschutzrechtlichen Fragen, die z. B. die Technik betreffen. Die Bundesdatenschutzbeauftragte hat unser Informations- und Einbindungsinteresse wohlwollend zur Kenntnis genommen. Inzwischen hat sie uns mitgeteilt, dass sie unser Anliegen in die Datenschutzkonferenz (DSK) eingebracht habe. In der Beratung sei bislang offen geblieben, in welchen Fällen und in welcher Art und Weise die Einbindung der spezifischen Aufsichtsbehörden stattfinden soll. In der 95. Sitzung der DSK soll dazu ein Vorschlag erarbeitet werden.

IV. Teilnahme an Fortbildungen und Veranstaltungen

In 2016 habe ich folgende Veranstaltungen besucht:

- 29./30.08.2016 Basisseminar des TÜV Rheinland „IT-Grundlagen für Datenschutzbeauftragte
- 13./14.06.2016 18. Computas-Fachkonferenz
- 15.06.2016 rbb-Inhouse-Schulung zum Thema „Compliance“
- 01.12.2016 Veranstaltung der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) zum Thema "EU-Datenschutz versus Medien- und Informationsfreiheit".

In 2017 habe ich an folgenden Veranstaltungen teilgenommen:

- 30.01.2017 Europäischer Datenschutztag (Zentrale Veranstaltung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder) „Diktatur der Daten? – Privatsphäre und Selbstbestimmung im Zeitalter von Big Data und Algorithmen“
- 20.04.2017: Veranstaltung der Vertretung der Europäischen Kommission in Deutschland, der Stiftung Datenschutz und der Berliner Datenschutzrunde „Datenschutz in Europa“ – Umsetzung der Datenschutzgrundverordnung, EU-US Datenschutzschild, Bekämpfung illegaler Hetze im Internet“
- 02.05.2017: TÜV Rheinland „Datenschutzgrundverordnung“
- 17./18.05.2017: Euroforum Datenschutzkongress Berlin
- 10.01.2018 Veranstaltung der Stiftung Datenschutz „Die ePrivacy-Verordnung – Wo stehen wir?“

Sämtliche Veranstaltungen fanden in Berlin statt.

Berlin, März 2018
gez. Anke Naujock

Anlagen

Anlage 1

Stellungnahme des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) zur möglichen Einführung von Office 365 in der Europa-Cloud

I. Management Summary

Derzeit gibt es in mehreren öffentlich-rechtlichen Rundfunkanstalten Überlegungen zur Einführung von Office 365 in der Europa-Cloud-Variante. Der AK DSB wurde mit Blick auf diese Entwicklung gebeten zu prüfen, ob es datenschutzrechtlich möglich ist, Office 365 in der Variante der Europa- Cloud in den Rundfunkanstalten einzuführen.

Aus Sicht des AK DSB würde mit einem solchen Umstieg ein Paradigmenwechsel begangen. Es würde im großen Umfang die Verarbeitung von Unternehmensdaten und personenbezogenen Daten in die Hände eines Dritten und in die Cloud gegeben. Dies ist mit datenschutzrechtlichen Risiken verbunden. Aufgrund der Tragweite des damit verbundenen Systemwechsels und der entsprechenden Risiken handelt es sich dabei aus Sicht der Datenschutzbeauftragten um eine Managemententscheidung, bei der die datenschutzrechtlichen Risiken unbedingt berücksichtigt werden müssen.

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten sehen insbesondere folgende **datenschutzrechtliche Risiken:**

- Mit der Einführung der Europa-Cloud besteht ein erhöhtes **Risiko des Zugriffs Dritter** auf die Daten der Sender. Dieses resultiert daraus, dass zum einen auch bei einer Europa-Cloud keine strenge Lokalisierung der Daten auf europäische Server stattfindet, sondern auch hier Daten außerhalb des europäischen Rechtsraumes verarbeitet werden. Zum anderen werden die Daten durch ein US-amerikanisches Unternehmen mit Hauptsitz in den USA verarbeitet. Damit einher geht eine gesteigerte Möglichkeit des Zugriffs auf unsere Daten durch ausländische und US-amerikanische Behörden, wie Geheimdienste und Strafverfolgungsbehörden (Stichwort: Prism u. a.). Diese Risiken sind aus Sicht des Datenschutzes insbesondere relevant für die Verarbeitung von investigativen journalistischen Informationen, aber auch für sensible personenbezogene Daten von Mitarbeitern und Dritten. Der Schutz der sensiblen journalistischen Recherchedaten ist Kernaufgabe des öffentlich-rechtlichen Rundfunks. Er ist elementarer Bestandteil und gleichzeitig Voraussetzung der Rundfunkfreiheit und darf durch die Einführung von Office 365 in der Cloud nicht gefährdet werden.

- Datenschutzrechtlich relevant ist darüber hinaus, dass die **Kontrolle** über die Datenverarbeitung in einem solchen Modell **in großem Umfang in die Hände eines Dritten gelegt** wird. Auch hierin besteht ein Systemwechsel. Wie letztendlich genau die Datenverarbeitung durch Microsoft erfolgt, ist nur schwer nachzuhalten. Hier sind die Sender weitgehend angewiesen auf Informationen, die von Microsoft über Internetseiten zur Verfügung gestellt werden, die kontinuierlich angepasst werden, auf mündliche Aussagen bzw. auf Testate und Zertifizierungen. Letztendlich verlangt das Modell daher auch, dass man dem Vertragspartner nach der gebotenen sorgfältigen Prüfung vertraut. Ein großes Stück der Kontrolle gibt man in diesem Modell ab.

- Außerdem besteht ein datenschutzrechtliches Risiko in der **Datenverarbeitung außerhalb von Europa**, die auch in der Europa-Cloud-Variante stattfindet. Auch hier wird nur für einen Teil der Daten (die „ruhenden Daten") eine Speicherung in Europa garantiert. Dies birgt insofern ein Problem, als die Datenverarbeitung au-

ßerhalb von Europa nur unter bestimmen rechtlichen Voraussetzungen zulässig ist. Die hier derzeit zur Verfügung stehenden Rechtsinstrumente (Stichwort: Privacy Shield, Standardvertragsklauseln) sind jedoch datenschutzrechtlich umstritten. Es besteht die Gefahr, dass sie gerichtlich aufgehoben werden. In diesem Fall würde die Rechtsgrundlage für eine Verarbeitung von personenbezogenen Daten außerhalb des EWR entfallen. Die Daten müssten zurückgeholt werden.

- Außerdem ist das Risiko der **Verfügbarkeit der Daten** zu betrachten. Mit Einführung von Office 365 in der Europa-Cloud werden wesentliche Funktionalitäten wie z. B. E-Mail in die Cloud ausgelagert. Bei einem Zusammenbruch der Leitungsverbindung stünden sie nicht mehr zur Verfügung.

Aufgrund dieser Risiken sollte vor der Entscheidung für eine Europa-Cloud-Variante geprüft werden, ob – wenn die Sender zu dem Ergebnis kommen, dass eine Auslagerung der Datenverarbeitung unverzichtbar ist – auch ein Betrieb von Office 365 in Deutschland im besten Fall mit Ausschluss eines Datentransfers in die USA (z. B. in der sog. Private Cloud der Telekom) für die Rundfunkanstalten ein gangbarer Weg sein kann.

Sollten die Rundfunkanstalten nach Abwägung aller Vorteile und Risiken dennoch zu dem Ergebnis kommen, Office 365 mit der Europa-Cloud einführen zu wollen, so ist dies nur unter folgenden **datenschutzrechtlichen Voraussetzungen** möglich:

1. Microsoft muss tatsächlich *und vertraglich* die Einhaltung der erforderlichen technischen Sicherheitsmaßnahmen garantieren, um die Sicherheit der Daten zu gewährleisten. Dies ist durch entsprechende Testate (z. B. C 5 Zertifizierung nach BSI) nachzuweisen. Insoweit wird auch auf die Prüfungen der IT-Sicherheitsbeauftragten verwiesen.
2. Auch bei Office 365 ist zu gewährleisten, dass hoch vertrauliche personenbezogene Daten, insbesondere vertrauliche investigative Recherchedaten nicht in der Cloud verarbeitet werden und die Möglichkeit der lokalen Speicherung auch weiterhin technisch gewährleistet wird. Dies setzt voraus, dass in den Häusern eine entsprechende Informationsklassifizierung vorgenommen wird und eine Festlegung erfolgt, wie mit vertraulichen Daten umzugehen ist.
3. Es ist ein Auftragsdatenverarbeitungsvertrag (unter der DS-GVO Auftragsverarbeitungsvertrag) abzuschließen, der den Vorgaben der DS-GVO entspricht und die datenschutzrechtlichen Verantwortlichkeiten sowie die Kontrollrechte der Sender regelt.
4. Neben dem Auftragsdatenverarbeitungsvertrag sind zusätzlich die von der Europäischen Kommission genehmigten Standardvertragsklauseln abzuschließen.
5. Für den Fall, dass die derzeit bestehenden rechtlichen Instrumentarien, die eine Datenverarbeitung außerhalb des europäischen Rechtsraums ermöglichen, für unzulässig erklärt werden, ist die Rückholbarkeit der Daten zu gewährleisten.

II. Rahmenbedingungen der Prüfung des AK DSB

Basis der datenschutzrechtlichen Bewertung waren die von Microsoft zur Verfügung gestellten Unterlagen, die von den Anstalten übermittelten Informationen zu den Plänen der Sender sowie Informationen aus den Gesprächen mit Microsoft. Dabei ist darauf hinzuweisen, dass die von den Anstalten selbst übermittelten Anforderungen bis zuletzt insoweit lückenhaft waren, als die Bedarfe der Anstalten nur unkonkret formuliert wurden. Insbesondere erfolgte keine Konkretisierung der Kategorien bzw. der Arten personenbezogener Daten, die verarbeitet werden sollen. Auch ein Schutzbedarf für die in der Anwendung bzw. Cloud zu verarbeitenden Daten wurde nicht festgelegt. Da die sicherheitstechnischen und datenschutzrechtlichen Anforderungen jedoch stets abhängig sind vom Schutzbedarf der zu verarbeitenden Daten ist eine wesentliche Voraussetzung für eine abschließende Beurteilung bis heute nicht erfüllt.

Die vorliegende Stellungnahme enthält daher neben der Darstellung der rechtlichen Rahmenbedingungen auch Vorgaben zur Umsetzung, die nach Auffassung der Datenschutzbeauftragten von ARD, ZDF und DR bei der Einführung von Office 365 in der Cloud gegeben sein müssen.

Die Datenschutzbeauftragten weisen ausdrücklich darauf hin, dass sich ihre datenschutzrechtliche Bewertung ausschließlich auf die in Diskussion befindliche Cloud-Nutzung bezieht. Sie beinhaltet keine Prüfung und Bewertung der einzelnen Office 365-Anwendungen/-Module und deren spezifischen Datenverarbeitung. Sollten sich die Sender für eine Einführung von Office 365 entscheiden, ist für die jeweils einzelnen Module und die darin stattfindende konkrete Datenverarbeitung eine separate Bewertung erforderlich, die auch ein IT-Sicherheitskonzept für die konkret geplante Cloud-Nutzung umfassen muss.

III. Datenschutzrechtliche Bewertung der Verarbeitung von personenbezogenen Daten in der Europa-Cloud von Microsoft im Rahmen von Office 365

1. Grundlagen der datenschutzrechtlichen Bewertungen

Basis einer datenschutzrechtlichen Bewertung der Cloud-Nutzung ist der grundsätzliche Umgang mit personenbezogenen Daten in der Cloud. Dieser soll im Folgenden zunächst dargestellt und sodann rechtlich eingeordnet werden.

2. Allgemeines und Umgang mit personenbezogenen Daten

a.) Vertragliche Situation

Bei einer Wahl der Europa-Cloud schließt die Rundfunkanstalt die vertraglichen Vereinbarungen ausschließlich mit Microsoft. Nach aktueller Rechts- und Vertragslage wird ein Grundvertrag einschließlich Auftragsdatenverarbeitungsvertrag zwischen dem Sender und Microsoft Irland geschlossen. Parallel dazu erfolgt der Abschluss von Standardvertragsklauseln zwischen dem Sender und Microsoft USA.

b.) Ort der Datenverarbeitung

Nach den dem AK DSB vorliegenden Informationen erfolgt eine Verarbeitung von personenbezogenen Daten bei der Nutzung der sog. Europa-Cloud ***innerhalb und außerhalb von Europa***, d. h. europäischen Rechenzentren. Eine vollständige Beschränkung der Verarbeitung auf europäische Rechenzentren sagt Microsoft lediglich für die sog. **„ruhenden Daten“** zu. Was darunter zu verstehen ist, wird in den dem AK DSB vorliegenden Unterlagen

vertraglich nicht eindeutig definiert. Es ist jedoch davon auszugehen, dass von dem Begriff all diejenigen Daten erfasst werden, die sich nicht in Bearbeitung oder im Transport befinden. Nach dem derzeitigen Kenntnisstand ist davon auszugehen, dass sowohl die personenbezogenen Daten des **Active Directory**, als auch personenbezogene Daten im **Supportfall** und **Daten im Transfer** (Daten, die beim Zugriff auf die Cloudanwendungen vom Arbeitsplatz zur Cloud, bzw. umgekehrt transportiert werden) nicht ausschließlich in Europa, sondern zumindest auch in den USA verarbeitet werden. Korrekt wäre daher nicht von Europa-Cloud zu sprechen, sondern vielmehr von einer Global-Cloud, mit der präferierten Lokalisierung eines Teils der Daten in der Europäischen Union.

3. Datenschutzrechtliche Bewertung

a.) Erforderlichkeit des Abschlusses eines Auftrags*daten*verarbeitungsvertrages

Die datenschutzrechtliche Bewertung der Einführung von Office 365 in der Europa-Cloud muss anhand der Regelungen der DS-GVO erfolgen, die ab Mai 2018 Gültigkeit erlangt, da eine Einführung nach diesem Zeitpunkt ins Auge gefasst wird. Grundsätzlich ist es auch unter der DS-GVO möglich im entsprechenden Umfang personenbezogene Daten durch einen Dienstleister wie im Falle von Office 365 verarbeiten zu lassen, wenn ein entsprechender Auftragsdatenverarbeitungsvertrag (Art. 28 DS-GVO) abgeschlossen wird. Dieser regelt die Verantwortlichkeiten zwischen den beiden Parteien beim Umgang mit personenbezogenen Daten. Er legt u. a. fest, dass der Auftragnehmer – hier Microsoft als Auftragsverarbeiter– die Daten ausschließlich im Auftrag der Rundfunkanstalten verarbeiten darf. Microsoft ist zum Abschluss eines solchen Vertrages verpflichtet und bereit. Die Datenschutzbeauftragten gehen aufgrund der bislang geführten Gespräche und den gesichteten Unterlagen davon aus, dass es im Rahmen der konkreten Vertragsverhandlungen gelingen wird, hier datenschutzkonforme Verträge abzuschließen. Abschließend beurteilt werden kann dies jedoch erst bei Vorlage der Vertragsentwürfe.

b.) Grundsatz der Verarbeitung von personenbezogenen Daten innerhalb des Europäischen Wirtschaftsraumes

Die DS-GVO enthält wie auch die bislang geltenden datenschutzrechtlichen Regelungen den Grundsatz, dass personenbezogene Daten grundsätzlich nur im Geltungsbereich des Europäischen Datenschutzrechts verarbeitet werden. Eine Verarbeitung von personenbezogenen Daten außerhalb dieses Geltungsbereichs ist nur in Ausnahmefällen möglich, wenn gewährleistet wird, dass bei der Verarbeitung auch außerhalb des EWR-Raumes ein vergleichbares Datenschutzniveau besteht.

c.) Voraussetzungen für eine Datenverarbeitung außerhalb des EWRs nach der DS-GVO

Ein angemessenes Datenschutzniveau kann auf unterschiedliche Art und Weise gewährleistet werden, nämlich wenn

- die EU-Kommission die Angemessenheit in dem „Empfangsland" durch Beschluss festgestellt hat (Angemessenheitsbeschluss der EU-Kommission, z. B. Privacy Shield für Datentransfer in die USA; Art. 45 DS-GVO);
- geeignete Garantien vorliegen dafür, dass die Rechte der Betroffenen nicht eingeschränkt werden (z. B. Vereinbarung von Standardvertragsklauseln; Art. 46 DS-GVO)
- Ausnahmen für bestimmte Fälle gegeben sind (Art. 49 DS-GVO).

d.) Herangehensweise von Microsoft bei Office 365 in der Europa-Cloud zur Absicherung des Datentransfers in die USA

Microsoft versucht diesen datenschutzrechtlichen Anforderungen auf zwei Wegen gerecht zu werden: Zum einen haben sie sich den Regelungen des Privacy Shield unterworfen und zum anderen schließen sie mit ihren Kunden neben einem Auftragsdatenverarbeitungsvertrag die von der Europäischen Kommission genehmigten Standardvertragsklauseln ab.

e.) Rechtliche Problematik des Privacy Shield

Die EU-Kommission hat für das US-Privacy Shield in einem Angemessenheitsbeschluss (zukünftig Art. 45 DS-GVO) festgestellt, dass bei einer Datenverarbeitung durch US-Firmen in den USA ein angemessenes Datenschutzniveau gegeben ist, wenn sie sich den Regelungen des Privacy Shield unterworfen haben. Allerdings ist das Privacy Shield aus Datenschutzsicht hoch umstritten und wird auch bereits gerichtlich angefochten. Ob es der gerichtlichen Überprüfung standhält, ist stark zu bezweifeln. Zwar schafft es gegenüber dem vom EuGH gekippten Safe Harbor-Abkommen verbesserte Datenschutzbedingungen. Es ist allerdings äußerst fraglich, ob diese ausreichend sind. Vor diesem Hintergrund ist von einem umfangreichen und dauerhaft geplanten Datentransfer in die USA wie im Rahmen von Office 365 geplant ausschließlich auf Basis des Privacy Shields unbedingt abzuraten.

f.) Rechtliche Problematik der Standardvertragsklauseln

Aber auch eine Rechtfertigung des Datentransfers in die USA auf Basis von sog. Standardvertragsklauseln birgt datenschutzrechtliche Risiken. In 2001 hat die EU-Kommission durch Beschluss festgestellt, dass unter Verwendung der Standardvertragsklauseln eine Datenverarbeitung außerhalb des EWR-Raums grundsätzlich stattfinden kann. Die vertraglichen Regelungen, so der Schluss der EU-Kommission, bieten ausreichende Garantien für einen datenschutzkonformen Umgang mit personenbezogenen Daten. Dabei regeln die Vertragsparteien in den Standardvertragsklauseln u. a. ihre jeweiligen Verpflichtungen zur Einhaltung des Datenschutzes zum Umgang mit Beschwerden von Betroffenen zur Information über Anfragen Dritter einschließlich Behörden und zur Kontrolle durch die Aufsichtsbehörden.

Mit Blick auf die Entwicklungen in den USA, insbesondere den Erkenntnissen zum Vorgehen der Geheimdienste und nicht zuletzt auch im Hinblick auf das Vorgehen der Regierung von Donald Trump werden auch die Standardvertragsklauseln zunehmend hinterfragt. Auch hier findet derzeit eine gerichtliche Überprüfung vor den Gerichten in Irland statt (Max Schrems, der Kläger des Safe Harbor-Verfahrens, hatte die Irische Datenschutzaufsichtsbehörde wegen der Datenverarbeitung durch Facebook in den USA angerufen. Daraufhin hat die Datenschutzaufsichtsbehörde Facebook vor den ordentlichen Gerichten verklagt mit der Argumentation, die Verwendung von Standardvertragsklauseln garantiere keinen angemessenen Datenschutz). Im Zuge dieses Verfahrens wird auch der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsverfahrens angerufen werden. Die Vorlagefragen werden gegenwärtig formuliert. Die Standardvertragsklauseln bieten damit zwar gegenwärtig eine rechtliche Basis zur Datenverarbeitung außerhalb des EWR. Der Fortbestand dieses Rechtsinstruments ist jedoch nicht garantiert.

g.) Vertraulichkeit der Daten und Zugriff durch US-Behörden

Jenseits dieser rechtlichen, die Rechtsgrundlage des Datentransfers betreffenden Risiken, besteht außerdem das Risiko, dass die Daten bei Microsoft nicht vertraulich behandelt werden. Insbesondere zu betrachten ist hier der

Zugriff durch Dritte, insbesondere auch US-amerikanische Behörden. Zum einen steht hier die sicherlich schwer zu beurteilende Möglichkeit des Datenzugriffs durch US-Geheimdienste im Raum. Zum anderen ist bis heute nicht abschließend gerichtlich geklärt, ob nach US-amerikanischem Recht in Europa gespeicherte Daten vor einer Herausgabe an US-amerikanische Strafverfolgungsbehörden wirksam geschützt sind. Derzeit ist beim US-Supreme Court ein Verfahren anhängig in dem zu entscheiden ist, ob Microsoft E-Mail-Korrespondenz, die auf seinen Servern in der EU gespeichert ist, aufgrund eines Beschlagnahmebeschlusses an die Strafverfolgungsbehörden herausgeben muss. Nachdem Microsoft das Berufungsverfahren für sich und gegen eine Herausgabe entscheiden konnte, ist der Ausgang der Revision derzeit noch offen.

h.) Eingeschränkte Kontrollmöglichkeiten

Schlussendlich geht die Einführung von Office 365 in der Europa-Cloud mit einer grundsätzlichen Einschränkung der Kontrollmöglichkeiten einher. Unabhängig von dem datenschutzrechtlich erforderlichen und vertraglich zu vereinbarenden Kontrollrechts, sind die Möglichkeiten der Kontrolle beschränkt auf die Informationen, die Microsoft seinen Kunden zur Verfügung stellt und solchen die in Testaten oder Zertifikaten ggfs. auch von Dritten bescheinigt werden. Dabei haben die bisherigen Gespräche mit Microsoft gezeigt, wie schwierig es ist jenseits von Verweisen auf wechselnde Informationen auf Internetplattformen verbindliche Aussagen von Microsoft zu konkreten Datenverarbeitungsprozessen zu bekommen.

IV. Besondere Vorgaben für die Verarbeitung von personenbezogenen Daten in der Cloud aus Sicht der Datenschutzbeauftragten von ARD und ZDF

Sollten sich die Rundfunkanstalten entscheiden, Office 365 in der Variante der Europa-Cloud einzuführen, so ist dies aus Sicht der Datenschutzbeauftragten angesichts der oben beschriebenen Rechtslage und der bestehenden Risiken nur unter den folgenden Voraussetzungen möglich:

1. Keine hochvertraulichen Daten insbesondere zu investigativen Recherchen in der Cloud

Die o. g. Ausführungen haben die datenschutzrechtlichen Risiken aufgezeigt. Vor diesem Hintergrund sollte aus Sicht der Datenschutzbeauftragten von einer Verarbeitung von hoch vertraulichen, bzw. sensiblen personenbezogenen Daten in der Cloud abgesehen werden. Dies gilt neben sensiblen Mitarbeiterdaten insbesondere auch für besonders schützenswerte Informationen und personenbezogene Daten aus investigativen Recherchen. Eine Speicherung dieser Daten außerhalb des europäischen Datenschutzrechtsraumes ist aus Sicht der Datenschutzbeauftragten nicht vertretbar. Der Schutz der sensiblen journalistischen Recherchedaten ist Kernaufgabe des öffentlich-rechtlichen Rundfunks. Er ist elementarer Bestandteil und gleichzeitig Voraussetzung der Rundfunkfreiheit. Auch bei Einführung von Office 365 in der Cloud-Variante ist zu gewährleisten, dass eine On-Premise-Verarbeitung solch sensibler und besonders schützenswerter Daten auch weiterhin gewährleistet wird.

2. IT-Sicherheitsanforderungen

Nach der DS-GVO (insbesondere Art. 5, Abs. 1 f) und Art. 32 DS-GVO) sind personenbezogene Daten so zu verarbeiten, dass eine angemessene Sicherheit gewährleistet wird. Es ist die Integrität und Vertraulichkeit der Daten sicherzustellen, d. h. insbesondere auch der Schutz vor dem unbefugten Zugriff und/oder Manipulation durch Dritte zu gewährleisten. Dazu ist es erforderlich, dass Sicherheits-

maßnahmen umgesetzt und vertraglich auch zugesichert werden, die dem Stand der Technik[1] und den Schutzbedarf der Daten entsprechen. Insoweit wird auf die Prüfung der AG ITS verwiesen.

3. **Rückholbarkeit der Daten**
   Aufgrund der dargestellten datenschutzrechtlichen Risiken betreffend die Rechtsgrundlage einer Datenverarbeitung außerhalb des EWR ist auf eine Rückholbarkeit der Daten zu achten. Bei Ausgestaltung der Verträge ist zudem eine Regelung aufzunehmen, die eine Anpassung an geänderte rechtliche Voraussetzung ermöglicht.

4. **ADV-Vertrag und Standardvertragsklauseln**
   Wie beschrieben muss ein Auftrags*daten*verarbeitungsvertrag von Standardvertragsklauseln abgeschlossen werden, die den Anforderungen der DS-GVO entsprechen. Nach Prüfung der bislang von Microsoft vorgelegten Unterlagen und den geführten Gesprächen gehen die Vertreter des AK DSB davon aus, dass durch den Abschluss eines entsprechenden Auftragsdatenverarbeitungsvertrages und die Vereinbarung von Standardvertragsklauseln datenschutzkonforme Verträge abgeschlossen werden können. Eine detaillierte Prüfung und abschließende Bewertung kann allerdings erst mit Vorlage der tatsächlichen Vertragsentwürfe vorgenommen werden.

[1] z. B. Standard-Absicherung nach IT-Grundschutz

Anlage 2

LEITLINIEN ZUM DATENSCHUTZ IN DEN TELEMEDIEN- UND SOCIAL-MEDIA-ANGEBOTEN DER RUNDFUNKANSTALTEN

Herausgeber: Arbeitskreis der Datenschutzbeauftragten
von ARD, ZDF und Deutschlandradio

Inhalt

4 Vorbemerkung
5 Datenschutz „Basics"
10 Apps
15 Auftragsvergabe an Dritte
18 Chats, Foren, Gästebücher, Kommentarfunktionen
21 Cookies
24 Datenschutzerklärung
28 Drittplattformen
30 Embedding von fremden Inhalten: Plugins, Videos & Co
34 Gewinnspiele
37 Instant Messaging
39 Mailkontakt, Kontaktformular, Newsletter
42 Minderjährigen-Datenschutz
45 Personalisierung
48 Social Login
50 Standortdaten
53 Votings
56 Web-Analyse

VORBEMERKUNG

Was will Datenschutz?

Datenschutz ist ein Grundrecht, das die Privatsphäre schützt.

Freie Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Verarbeitung und Weitergabe seiner personenbezogenen Daten voraus. Datenschutz ist das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (sog. Recht auf informationelle Selbstbestimmung). Geschützt wird damit die Freiheit des Einzelnen, selbst zu entscheiden, wer was wann und bei welcher Gelegenheit über ihn weiß. Das Internet und die zunehmende Digitalisierung stellen den Datenschutz dabei vor neue Herausforderungen. Das Wachstum des Internets geht mit einem stetigen Anstieg der gesammelten personenbezogenen Daten einher.

Was will der Leitfaden?

Dieser Leitfaden ist ein Ratgeber und richtet sich an die Mitarbeiter[1], die Telemedien- und Social-Media-Angebote redaktionell einsetzen und technisch realisieren. Er konkretisiert die verbindlichen Vorgaben der Datenschutzgesetze und der einschlägigen Rechtsprechung für öffentlich-rechtliche Telemedien- und Social-Media-Angebote.

Der Leitfaden soll eine Orientierung bieten und den Telemedienverantwortlichen in den Rundfunkanstalten dabei helfen, datenschutzrelevante Themen zu erkennen, zu beurteilen und sie mit datenschutzrechtlichen Vorgaben verantwortungsvoll in Einklang zu bringen. Der Leitfaden ersetzt jedoch nicht die Beratung mit dem zuständigen Datenschutzbeauftragten, der im Zweifel hinzuzuziehen ist.

Der Leitfaden bietet mit den Datenschutz „Basics" einen Überblick über die wichtigsten datenschutzrechtlichen Grundprinzipien. Daneben liegt der Fokus auf praxisrelevanten Einzelthemen von A wie Apps bis W wie Webanalyse. Anhand von Checklisten wird dabei für jedes Thema dargestellt, worauf für eine datenschutzkonforme Realisierung zu achten ist. Oftmals sind hier neben dem Datenschutz noch andere rechtliche Aspekte zu beachten; diese sind in Rücksprache mit den zuständigen Justitiariaten zu klären.

1 Zur besseren Lesbarkeit wird im Folgenden ausschließlich eine Bezeichnungsform verwendet. Selbst-verständlich sind alle Formulierungen für alle Geschlechter gleichermaßen zutreffend.

DATENSCHUTZ „BASICS“

Welche Grundgedanken stehen hinter den Anforderungen, die der Datenschutz an die Rundfunkanstalten für ihre Telemedienangebote stellt? Mit ein paar Grundprinzipien kann man sich auch im komplizierten Datenschutzrecht gut zurechtfinden.

Sind die Daten personenbezogen?

Die Regelungen des Datenschutzrechts kommen nur dann zur Anwendung, wenn die Rundfunkanstalt „personenbezogene Daten“ von Nutzern speichert und nutzt.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Darunter versteht man alle Daten, die dazu genutzt werden können, die Identität des Users offen zu legen. Dazu gehören nicht nur der richtige Name, Anschrift, Telefonnummer oder eine E-Mail-Adresse. Auch andere Informationen wie z.B. die IP-Adresse, Standortdaten, Gerätekennungsnummern sowie sonstige Informationen (z.B. über das Nutzungsverhalten) sind ebenfalls relevant, weil sie zumindest personenbeziehbar sind.[2]

Wer ist die für die Datenverarbeitung „verantwortliche Stelle“?

Wenn die Rundfunkanstalt in ihren Telemedienangeboten personenbezogene Daten von Nutzern verarbeitet, ist sie gemäß den Datenschutzgesetzen die „verantwortliche Stelle“ und damit verantwortlich für die datenschutzkonforme Gestaltung ihrer Angebote.

Dies gilt auch, wenn sich die Rundfunkanstalt bei der Umsetzung einer Webseite, dem Hosting oder der App-Programmierung eines externen Dienstleisters bedient, der im Auftrag der Anstalt tätig wird (siehe hierzu die Hinweise zur ***Auftragsvergabe an Dritte***).

2 Aufgrund der aktuellen Rechtsprechung und im Einklang mit der Auffassung der deutschen Aufsichtsbehörden im Datenschutz sind statische und dynamische IP-Adressen als personen-bezogene Daten zu werten.

Sofern die Rundfunkanstalt in ihren Angeboten Tools und sonstige Inhalte von externen Dritten einbindet, bleibt sie jedenfalls insofern rechtlich verantwortlich, dass sie dafür sorgen muss, dass die Übertragung von Daten der Nutzer an Dritte mit dem Wissen und Wollen der Nutzer erfolgt (siehe hierzu die Hinweise zum ***Embedding von fremden Inhalten***).

Ist die Rundfunkanstalt auf einer Drittplattform präsent, ist grundsätzlich der jeweilige Plattformanbieter für die Datenverarbeitung datenschutzrechtlich verantwortlich (siehe hierzu die Hinweise zu ***Drittplattformen***).[3]

Rechtmäßigkeit der Datenerhebung und -nutzung

Werden personenbezogene Daten gespeichert und verarbeitet, bedarf dies stets einer Erlaubnis. Eine solche Erlaubnis kann sich entweder aus einer Rechtsvorschrift, einem Vertrag oder aus einer ausdrücklichen Einwilligung des Nutzers ergeben.

Die datenschutzrechtliche Zulässigkeit der Datenverarbeitung lässt sich nicht pauschal beurteilen, sondern muss anhand des jeweiligen Einzelfalls geprüft werden.

Der Leitfaden gibt für verschiedene typische Fragestellungen eine Orientierung, was die Rundfunkanstalten zu beachten haben.

Einwilligung des Nutzers

Sofern die Erhebung von personenbezogenen Daten nicht per Gesetz erlaubt ist, ist grundsätzlich eine Einwilligung des Nutzers notwendig. Für eine wirksame Einwilligung ist auf folgendes zu achten:

» Der Nutzer ist vor Beginn der Datenverarbeitung umfassend zu informieren.

» Der Text der Einwilligungserklärung muss dem Nutzer klar und allgemein verständlich über die zu

3 Aufgrund der aktuellen Rechtsprechung ist davon auszugehen, dass auch der Betreiber einer Facebook-Fanpage keine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist.

verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die Rundfunkanstalt informieren.

» Der Einwilligungstext muss klar und eindeutig formuliert sein, so dass der Nutzer erkennen kann, was er hier erklärt („Ich willige ein, dass ...“; „Ich bin einverstanden, dass ...“).

» Es muss sich um eine bewusste Erklärung handeln (Opt-in). Diese kann z.B. im Wege eines Häkchens in einer Checkbox abgegeben werden. Aber: Im Sinne einer Zustimmung vorangekreuzte Einwilligungstexte oder nur mit einer Streich-/Abwahl-Möglichkeit versehene „vorgegebene“ Zustimmungen (Opt-out) genügen nicht.

» Sollen besonders sensible persönliche Daten erhoben und verarbeitet werden, ist der Nutzer darüber im Zuge seiner Einwilligung gesondert zu unterrichten. Dies ist z.B. der Fall bei: Angaben über die ethnische Herkunft; politische Meinungen; religiöse und philosophische Überzeugungen; Daten zu Gesundheit und Sexualleben; Daten über Straftaten.

» Eine wirksame Einwilligung liegt nur vor, wenn diese freiwillig abgegeben wird. Eine unter Druck oder Zwang abgegebene Einwilligung ist unwirksam.

» Wird eine Einwilligung elektronisch im Rahmen eines Telemedienangebotes eingeholt, muss die Einwilligung protokolliert werden und jederzeit für den Nutzer abrufbar sein. Es ist ausreichend, wenn die Einwilligung jeweils auf Anfrage zugänglich gemacht wird.

» Die Einwilligung muss jederzeit in einfacher Weise vom Nutzer widerrufbar sein. Der Nutzer ist über sein Widerrufsrecht zu informieren. Die Unterrichtung kann z.B. in der allgemeinen ***Datenschutzerklärung*** erfolgen.

» Die datenschutzrechtliche Einwilligung zu einer konkreten Datenverarbeitung ist deutlich zu trennen von den generellen Datenschutzhinweisen in einem Telemedienangebot mit reinen Informationen über Datenverarbeitung auf gesetzlicher Grundlage (siehe hierzu die Hinweise zur ***Datenschutzerklärung***).

» Besonderheiten gelten bei der Datenverarbeitung von Minderjährigen (Hinweise zum ***Minderjährigen-Datenschutz***).

Grundsatz der Zweckbindung und Erforderlichkeit

Jeder Umgang mit personenbezogenen Daten muss einen ganz bestimmten Zweck verfolgen. Die Daten dürfen nur gespeichert und verarbeitet werden, soweit diese Verarbeitung für den jeweiligen Zweck erforderlich ist. Eine pauschale Abfrage und Nutzung von persönlichen Daten eines Nutzers ohne Verfolgung eines konkret festgelegten Zwecks ist daher nicht zulässig. Eine Verwendung der Daten für andere Zwecke ohne Wissen und Einverständnis des Nutzers ist ebenfalls nicht zulässig.

Sobald die personenbezogenen Daten nicht mehr zu dem ursprünglich angegebenen Zweck

benötigt werden, müssen sie grundsätzlich gelöscht werden. Das gleiche gilt im Falle des Widerrufs einer Einwilligungserklärung in die Datenverarbeitung durch den Nutzer.

Aber: Unabhängig vom Datenschutz können gesetzliche Aufbewahrungspflichten bestehen (z.B. nach den Vorgaben der Abgabenordnung oder des Handelsgesetzbuches). In diesem Fall sind die Daten zu sperren und damit von den aktuellen Produktivdaten zu trennen.

Grundsatz der Datenvermeidung und Datensparsamkeit

Es sollen immer so wenig personenbezogene Daten wie möglich für den konkreten Zweck abgefragt werden. Dabei hilft die Kontrollfrage: Wozu brauchen wir diese Daten?

Diesem Ziel kann auch eine Pseudonymisierung oder Anonymisierung von Daten dienen. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (i.d.R. eine mehrstellige Buchstaben- oder Zahlenkombination, auch Hash genannt) ersetzt, um die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren. Die Anonymisierung ist das Verändern personenbezogener Daten derart, dass diese Daten überhaupt nicht mehr einer Person zugeordnet werden können.

Soweit es der Rundfunkanstalt technisch möglich und zumutbar ist, hat sie die Nutzung ihrer Telemedienangebote anonym oder unter Pseudonym zu ermöglichen.

„Privacy by Design" und „Privacy by Default"

Die Rundfunkanstalt sollte bereits in der Entstehungs- und Entwicklungsphase von Webseiten, Apps oder bei ihrer Präsenz auf Drittplattformen den datenschutzrechtlichen Vorgaben Rechnung tragen und durch datenschutzgerechte technische Gestaltung („Privacy by Design") sowie datenschutzfreundliche Voreinstellungen („Privacy by Default") dafür Sorge tragen, dass ihre Angebote datenschutzkonform sind. Der Datenschutz soll von vorneherein in die Gesamtkonzeption einbezogen werden anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme u.a. zu beheben. Dazu gehört auch, dass die Funktionalitäten standardmäßig datenschutzfreundlich voreingestellt sind.

Transparenz

Das Grundrecht auf informationelle Selbstbestimmung verlangt: Der Einzelne soll wissen, wer

was wann und bei welcher Gelegenheit über ihn weiß. Das Transparenzprinzip wirkt sich an vielen Stellen im Datenschutzrecht aus:

Die Anbieter einer Webseite oder App sind insbesondere verpflichtet, die Nutzer in einer Datenschutzerklärung über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über eine etwaige Weitergabe der Daten an Dritte in einer leicht verständlichen Weise zu informieren (vgl. hierzu die Hinweise zur ***Datenschutzerklärung***).

Im Rahmen der Einwilligung muss dargestellt werden, welche Daten zu welchen Zwecken erhoben werden. Auch nach der Erhebung hat der Einzelne bestimmte Nutzerrechte: Jeder Nutzer, dessen personenbezogene Daten durch die Rundfunkanstalt erhoben und verwendet werden, hat das Recht, Auskunft über die zu seiner Person gespeicherten Daten zu verlangen. Unter bestimmten Voraussetzungen kann er zudem die Berichtigung, Löschung und Sperrung von Daten verlangen.

Datensicherheit

IT-Systeme sind aufgrund ihrer Komplexität anfällig für Fehler, über die z.B. Unbefugte an Daten gelangen können. Gleichzeitig werden auch die Angriffe auf technische Systeme immer häufiger und ausgefeilter. Die Rundfunkanstalt hat daher gemeinsam mit dem IT-Sicherheitsbeauftragten und/oder der zuständigen Fachabteilung für ihre Webseiten und Apps geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Daten ihrer Nutzer gegen Verfälschung, Verlust und Missbrauch zu schützen.

APPS

Apps sind Applikationen, die an bestimmte Plattformen angepasst werden. Sie können als native und/oder hybride Apps z.B. für mobile Endgeräte (Smartphone, Tablet) und stationäre Geräte (Smart-TV, Apple-TV u.ä.) angeboten werden. Sie können Daten in großem Umfang erfassen und verarbeiten, um dem App-Nutzer neue und innovative Dienstleistungen anzubieten. Viele Arten von Daten, die auf Endgeräten gespeichert sind oder von diesen Geräten erstellt werden, sind personenbezogene Daten und unterliegen damit datenschutzrechtlichen Regelungen.

Was sagt der Datenschutz?

Die größten Datenschutzrisiken für Nutzer sind die mangelnde Transparenz und die mangelnde Kenntnis der von einer App auf der jeweiligen Plattform ausgeführten Verarbeitung personenbezogener Daten sowie das Fehlen einer expliziten Einwilligung des Nutzers vor der Verarbeitung. Unzureichende Sicherheitsmaßnahmen, ein Trend zur Datenmaximierung und die ungenaue Festlegung der Zwecke, für die personenbezogene Daten erfasst werden, erhöhen die Risiken bei Apps zusätzlich.

Die Rundfunkanstalt ist datenschutzrechtlich für die in einer von ihr angebotenen App anfallenden Nutzerdaten vollumfänglich verantwortlich. Dies gilt auch dann, wenn die App über den Server eines Dienstleisters betrieben wird.

Die Verarbeitung von Nutzerdaten durch die App-Store-Betreiber bei der Anmeldung zum Store und dem Herunterladen einer App liegt dagegen außerhalb der Verantwortung der Rundfunkanstalt.

Checkliste

Als App-Anbieter und -Entwickler hat die Rundfunkanstalt für eine datenschutzkonforme App auf Folgendes zu achten.

× Welche personenbezogenen Daten werden genutzt?

Apps und mobile Geräte enthalten bzw. erfassen Informationen, die auf den ersten Blick nicht immer als „personenbezogene Daten" im Sinne des Datenschutzrechts zu erkennen sind. Die Bestimmbarkeit einer Person im Zusammenhang mit mobilen Geräten und Apps ist insbesondere bei folgenden Informationen zu bejahen:

» IP-Adresse des Nutzers

» Standortdaten

» Kontakte

» Eindeutige Geräte- und Kartenkennungen

» Identität der betroffenen Person

» Name des Telefons (Nutzer neigen dazu, ihr Telefon unter Verwendung ihres eigenen Namens zu benennen, z.B. „Max Mustermanns iPhone")

» Kreditkarten- und Zahlungsdaten

» Anruflisten, SMS oder Instant Messaging

» Browserverlauf

» E-Mail

» Authentifizierungsdaten für spezielle Dienste, insb. Social Media

» Foto- und Filmaufnahmen einer Person; Audiodaten mit Stimmaufnahmen

× „Privacy by Design" und „Privacy by Default"

Die Rundfunkanstalt sollte bereits in der Entstehungs- und Entwicklungsphase einer App den datenschutzrechtlichen Vorgaben Rechnung tragen und durch datenschutzgerechte technische Gestaltung („Privacy by Design") sowie datenschutzfreundliche Voreinstellungen („Privacy by Default") Sorge tragen. Aus diesem Grund ist bereits bei der Entwicklung einer App darauf zu achten, dass durch diese später nur diejenigen personenbezogenen Daten erhoben und verwendet werden, welche für die Durchführung der gewünschten Funktion unbedingt erforderlich sind.

× Möglichkeit der anonymen und pseudonymen Nutzung

Soweit es möglich ist, sollte die Rundfunkanstalt die Nutzung ihrer App anonym oder unter

Pseudonym ermöglichen. Über diese Möglichkeit ist der Nutzer zu informieren. Achtung: Eindeutige Geräte- und Kartenkennungen oder die IP-Adresse stellen kein Pseudonym dar!

× Berechtigungen nur nach dem Grundsatz der Zweckbindung

Nach der Installation einer App müssen zur Erbringung des Dienstes in der Regel Berechtigungen bei dem Nutzer eingeholt werden, mittels derer die Rundfunkanstalt sowohl auf Funktionen des Gerätes als auch auf Daten, welche auf dem Gerät gespeichert sind, zugreifen kann.

Hier gilt: Es dürfen nur die für die App tatsächlich erforderlichen Berechtigungen vom Nutzer angefordert werden. Einige Betriebssysteme bieten Berechtigungen nur in festen Kombinationen an, welche neben der erforderlichen Berechtigung auch nicht benötigte Berechtigungen enthalten. Die Rundfunkanstalt muss in der Datenschutzerklärung über diesen Umstand aufklären und sich gegenüber dem Nutzer dazu verpflichten, von der nicht erforderlichen Berechtigung keinen Gebrauch zu machen.

× Es gilt: Grundsatz der Einwilligung

Sollen personenbezogene Daten (z.B. über entsprechende Formulare in der App) erhoben werden, so ist dazu grundsätzlich die ausdrückliche Einwilligung des Nutzers erforderlich (siehe hierzu die Hinweise zur Einwilligung in den ***Datenschutz „Basics"***).

× Erlaubt: Nutzung von Daten, die zur Inanspruchnahme der App notwendig sind

Ohne ausdrückliche Einwilligung darf die Rundfunkanstalt sog. Nutzungsdaten eines Nutzers erheben. Nutzungsdaten sind solche personenbezogenen Daten, welche notwendigerweise zur tatsächlichen Nutzung der App durch die Rundfunkanstalt erhoben und verwendet werden müssen (z.B. die IP-Adresse oder - soweit im Einzelfall erforderlich - eindeutige Kennnummern).

× Erlaubt: Pseudonyme Nutzungsprofile unter bestimmten Voraussetzungen

Grundsätzlich dürfen Nutzerdaten nur mit ausdrücklicher Einwilligung protokolliert werden. Aber: Zu Marktforschungszwecken (insb. Reichweitenmessung) können unter Beachtung bestimmter Voraussetzungen pseudonyme Nutzungsprofile erstellt werden.

Der Nutzer muss im Rahmen der Datenschutzerklärung auf die Erstellung des Nutzungsprofils und auf die Möglichkeit, der Erstellung zu widersprechen, hingewiesen werden. Dazu muss ihm eine direkte Opt-Out Möglichkeit (Aus-Schalter in den App-Einstellungen) zur Verfügung gestellt werden, welche mit einem Klick aktiviert werden kann. Der bloße Hinweis auf bestimmte Einstellungsmöglichkeiten am Gerät etc. genügt nicht. Widerspricht der Betroffene der Profilbildung unter Pseudonym, so sind etwa vorhandene Profildaten zu löschen oder wirksam zu anonymisieren (siehe hierzu die Hinweise zur ***Web-Analyse***).

× Push-Funktionen mit Zustimmung des Nutzers zulässig

Mit der Push-Funktion können verschiedene Inhalte - z.B. Kurznachrichten, Live-Ticker usw.

- von einem Server zu einem speziellen Mobilgerät versandt werden. Hat der Nutzer einmal den Dienst abonniert, übernimmt der Server eigeninitiativ das „Pushen" des Inhalts zum Nutzer-Device.

Damit die Rundfunkanstalt weiß, wer welche Push-Nachrichten möchte, ist eine eindeutige Kennung erforderlich. Es wird empfohlen, keine personenbezogene Nutzerdaten zu erheben, sondern mit einer zufallsgenerierten eindeutigen Nummer (sog. Token oder Device Token ID) zu arbeiten: Mit Zustimmung des Nutzers wird durch das Betriebssystem des Gerätes des Abonnenten ein Token generiert. Die Device Token ID wird an den Server übermittelt. So weiß die Rundfunkanstalt, an wen sie welche Push-Nachrichten schicken muss. Durch solche zufallsgenerierte Token wird die Möglichkeit der App-übergreifenden Nachverfolgung von Nutzern eingeschränkt.

Auf die Funktionalität der Device Token ID ist in der Datenschutzerklärung hinzuweisen.

× Achtung bei Standortdaten

Sofern durch die App auf Standortdaten des Geräts zugegriffen wird, muss darauf geachtet werden, dass dies nur im zulässigen Umfang geschieht. Hier sind die Hinweise zu ***Standortdaten*** zu beachten.

× Achtung beim Einbinden von Inhalten von Drittanbietern

Werden Inhalte von Drittanbietern in die App eingebunden, besteht die Gefahr, dass allein durch das Aktivieren der App Nutzerdaten ohne Wissen und Wollen des jeweiligen Nutzers an die Drittanbieter fließen.

Hier muss auf eine datenschutzkonforme Gestaltung geachtet werden. Mit Hilfe von Vorschaltseiten kann z.B. sichergestellt werden, dass die Nutzerdaten erst dann zu den Anbietern der eingebundenen Inhalte fließen, wenn der Nutzer zuvor entsprechend informiert worden ist im Rahmen der aus Datenschutzsicht gebotenen Zwei-Klick-Lösung (siehe hierzu die Hinweise zum ***Embedding von fremden Inhalten***).

× Umfassende spezifische Datenschutzerklärung vor Installation der App

Neben der Veröffentlichung eines Impressums hat die Rundfunkanstalt in einer eigenen Datenschutzerklärung in der App über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung der Nutzerdaten zu informieren. Was die wesentlichen Inhalte der Datenschutzerklärung sind, bestimmt sich anhand des Funktionsumfangs der App.

Wegen der beschränkten Display-Größe mobiler Endgeräte sind die Datenschutzhinweise so zu gestalten, dass der Nutzer jederzeit ohne großen Aufwand die gewünschten Informationen erhalten kann.

Eine einfache Verknüpfung mit der Datenschutzerklärung eines ähnlichen oder alternativen Webangebotes der Rundfunkanstalt genügt dann nicht, wenn es hinsichtlich der

Datenverarbeitung relevante Unterschiede bei der Datenverarbeitung einer Webseite und einer App gibt.

Die App-spezifische Datenschutzerklärung muss vor der Installation der App erfolgen. Die Datenschutzerklärung muss also entweder im App-Store als Link oder nach dem Herunterladen für den Nutzer zum Abruf bereitgehalten werden.

Um dem Nutzer die unkomplizierte Wahrnehmung seiner Nutzerrechte zu ermöglichen, ist eine einfache Kontaktmöglichkeit zum Datenschutzbeauftragten anzugeben.

× Auf Datensicherheit achten

Eine zentrale Rolle bei der datenschutzgerechten Gestaltung spielt die Sicherheit einer App. Insbesondere an folgendes ist zu denken:

» Sowohl beim Versand als auch beim Empfang von Daten zwischen Nutzer und Rundfunkanstalt sollte die Kommunikationsverbindung mit dem Backend durch eine Transportverschlüsselung abgesichert sein.

» Es sollten nur diejenigen personenbezogenen Daten lokal auf dem Gerät gespeichert werden, die unbedingt für den Betrieb der App notwendig sind. Auch die Speicherdauer muss sich an dieser Notwendigkeit orientieren. Bei einer Deinstallation der App muss sichergestellt werden, dass die lokal gespeicherten personenbezogenen Daten des Nutzers sowie die Cookies gelöscht werden.

» Sofern für das Nutzen der App eine eindeutige Kennung erforderlich sein sollte, wird empfohlen, eine zufallsgenerierte eindeutige Nummer (ein Token) zu erzeugen, die im Rahmen der App-Nutzung zwar eindeutig ist, außerhalb der App oder bei Neuinstallation jedoch keinen Bezug mehr zum Gerät bzw. Nutzer ermöglicht.

× Achtung bei Beauftragung von Dritten

Die Rundfunkanstalt ist datenschutzrechtlich vollumfänglich verantwortlich, wenn sie eine App anbietet. Dies gilt auch dann, wenn die App im Auftrag der Rundfunkanstalt von Dienstleistern entwickelt, programmiert oder gehostet wird oder sonstige Daten (z.B. Device Token ID) durch einen externen Dienstleister verarbeitet werden.

Falls ein Dritter mit der Entwicklung der App beauftragt ist, ist darauf zu achten, dass keine personenbezogenen Daten übertragen werden. Eine Erhebung und Verwendung personenbezogener Daten des Nutzers einer App ist auf Entwicklerseite in der Regel nicht erforderlich und müsste deshalb im Einzelfall begründet werden und von einem Erlaubnistatbestand gedeckt sein.

Im Übrigen gelten die Hinweise zur ***Auftragsvergabe an Dritte***.

× Minderjährigen-Datenschutz

Bei Apps speziell für Kinder und Jugendliche sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

AUFTRAGSVERGABE AN DRITTE

Vergibt eine Redaktion oder der für Web-Technik zuständige Fachbereich Aufträge an Dritte – z.B. für App-Programmierung oder das Programmieren von anderen Anwendungen, Hosting, Medienforschung usw. – und erhält bzw. verarbeitet dieser externe Dienstleister dabei personenbezogene Daten der Nutzer, müssen die gesetzlichen und hausinternen Regelungen zur Datenverarbeitung durch Dritte beachtet werden. In diesem Kontext gewinnen zunehmend auch „Cloud-Dienste", die von externen Unternehmen angeboten werden, an Bedeutung.

Was sagt der Datenschutz?

Vorab ist gemeinsam mit dem Datenschutzbeauftragten zu klären, ob es sich um eine sog. Auftragsdatenverarbeitung i.S. des Datenschutzrechts handelt.

Auftragsdatenverarbeitung (ADV) ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen externen Dienstleister im Auftrag der verantwortlichen Stelle – also der jeweiligen Rundfunkanstalt. In diesem Fall bleibt ausschließlich die Rundfunkanstalt für die Verarbeitung der Daten verantwortlich. Die Rundfunkanstalt hat die Zulässigkeit der Datenverarbeitung zu prüfen, die Erfüllung der Nutzerrechte zu gewährleisten und mögliche Haftungsrisiken zu tragen. Es gibt detaillierte gesetzliche Vorgaben, welche Rechte, Pflichten und Maßnahmen in diesem Fall durch eine gesonderte schriftliche Vereinbarung zwischen dem Auftraggeber (also der Rundfunkanstalt) und dem Dienstleister zu treffen sind. Ganz wesentlich ist dabei die Datensicherheit: Das Schutzniveau für die Daten muss mindestens dem Schutzniveau bei Abwicklung im eigenen Unternehmen entsprechen.

Checkliste

× Grundsätzlich: Bevorzugung einer „Inhouse"-Lösung

Eine Vergabe von Aufträgen an Externe ist grundsätzlich möglich. Die hohen datenschutzrechtlichen Maßstäbe für öffentlich-rechtliche Angebote können aber regelmäßig am besten durch die Rundfunkanstalt selbst realisiert und kontrolliert werden.

Sofern möglich, sollten die jeweiligen Nutzerdaten daher in der Rundfunkanstalt verarbeitet und gespeichert werden (z.B. Inhouse-Programmierung und dem Hosten der App auf anstaltseigenen Servern). Eine Durchführung durch externe Dritte sollte gegenüber einer anstaltsinternen Lösung nur nach Abwägung aller relevanten Aspekte bevorzugt werden.

× Vor Auftragsvergabe: Sind personenbezogene Daten betroffen?

Es ist vorab zu klären, ob der Dienstleister im Zusammenhang mit seinem Auftrag personenbezogene Daten von Nutzern erhält bzw. verarbeitet. Nur dann gelten die datenschutzrechtlichen Regelungen zur ADV. Die Einordnung ist nicht immer einfach. Sofern ein Auftrag an Dritte erfolgen soll, bei dem möglicherweise Nutzerdaten übermittelt werden, sollte im Zweifel die zuständige Beschaffungsstelle (z.B. der Einkauf), die IT-Sicherheit und/oder der Datenschutzbeauftragte eingebunden werden.

× Bei Auftragsdatenverarbeitung: Beachtung der anstaltsinternen Regelwerke

Sofern es sich um eine ADV handelt, sind die einschlägigen hausinternen Regelungen zu beachten. In einigen Rundfunkanstalten gibt es entsprechende Dienstanweisungen zur ADV oder formalisierte Abläufe und Mustertexte für die erforderliche Vereinbarung. In allen Fällen können die Beschaffungsstellen und der Datenschutzbeauftragte weiterhelfen.

× Hierauf ist besonders zu achten!

Einige Dienstleister arbeiten auch für private Anbieter und sind sich der besonders hohen datenschutzrechtlichen Standards für die Angebote der Rundfunkanstalten nicht immer bewusst. Oftmals ist für externe Dienstleister z.B. die Datenspeicherung außerhalb der EU üblich oder Dienstleister mit Sitz außerhalb der EU können auf Daten innerhalb der EU zugreifen. Für die Übermittlung/Verarbeitung von Daten in sog. Drittländer - d.h. Staaten außerhalb der EU - gelten besonders hohe Zulässigkeitsanforderungen; zudem sind zusätzliche datenschutzrechtliche Absicherungen erforderlich.

Einige Dienstleister implementieren für ihre kommerziellen Auftraggeber oder die eigenen Zwecke regelmäßig Tracking-Tools. Deshalb ist es wichtig, dass die Rundfunkanstalt die eigenen Anforderungen klar definiert und kommuniziert.

Es ist zu empfehlen, jede beauftragte Anwendung vor dem Ersteinsatz und nach Updates daraufhin zu testen, ob nicht doch - versehentlich und unbedacht - datenschutzrechtlich problematische Applikationen implementiert sind, die Daten an andere Dritte (z.B. Google oder Facebook usw.) übermitteln. Dies gilt auch dann, wenn der Auftrag selbst - z.B. die App-Programmierung - eigentlich nicht als ADV einzuordnen ist.

× Information über Verarbeitung von Nutzerdaten durch Dritte

Aus Gründen der Transparenz kann in der Datenschutzerklärung darüber informiert werden, dass die Rundfunkanstalt bei bestimmten Projekten durch Dritte unterstützt wird und dabei Nutzerdaten durch Dritte gespeichert oder verarbeitet werden.

Bei einer Erhebung und Nutzung von Nutzerdaten durch Dienstleister mit Sitz in einem Drittstaat außerhalb der EU/EWR und/oder mit Zugriff auf die Daten aus Drittstaaten muss hierüber in der Datenschutzerklärung informiert werden.

CHATS, FOREN, GÄSTEBÜCHER, KOMMENTARFUNKTIONEN

Kommentarfunktionen, Chats und andere interaktive Tools zum Austausch der Nutzer untereinander und zum Veröffentlichen eigener Inhalte wie z.B. Fotos oder Videos (sog. User Generated Content) sind mittlerweile gängiger Bestandteil öffentlich-rechtlicher Online-Angebote. Um sicherzustellen, dass diese Tools datenschutzkonform eingesetzt werden und der Austausch mit den Nutzern konstruktiv und angenehm bleibt, bedarf es klarer Regelungen und redaktioneller Begleitung.

Was sagt der Datenschutz?

Wer auf seiner Webseite Chats, Foren und andere interaktive Funktionen anbietet, verarbeitet Daten und Inhalte seiner Nutzer. In den meisten dieser Fälle müssen sich die Besucher registrieren oder zumindest eine E-Mail-Adresse angeben. Dadurch entsteht ein datenschutzrechtlich relevanter „Personenbezug". Interaktive Tools können aber auch so eingerichtet werden, dass jeder Besucher einen Beitrag ohne weitere Angaben veröffentlichen kann. Dabei ist aber zu bedenken, dass auch der Inhalt eines (vermeintlich) anonymen Beitrags einen Personenbezug im rechtlichen Sinne aufweisen kann. Rechtlich macht es daher fast keinen Unterschied, ob Nutzer sich registrieren müssen oder auch ohne weitere Angaben mitmachen können.

Die Kommentare der Nutzer können u.a. das Recht Dritter auf informationelle Selbstbestimmung verletzen: Das kann dann der Fall sein, wenn personenbezogene Daten wie Anschriften, E-Mail-Adressen und Telefonnummern in den Kommentaren veröffentlicht werden. Gleiches gilt für offenkundig private Korrespondenz, wie Briefe, E-Mails u.ä..

Checkliste

× Datenschutzrechtlich erforderliche Einwilligung des Nutzers

Es empfiehlt sich, für die Teilnahme an Chats, Foren u.a. eine aktive Einwilligung des Nutzers einzuholen (z.B. durch aktives Setzen eines Häkchens in der Checkbox). In der Regel fallen folgende Angaben an:

» die Beiträge der Nutzer selber,

» hinzu kommt in aller Regel ein Nutzername und oft auch ein Passwort sowie eine E-Mail-Adresse,

» auch bei einfachen Internetseiten fallen die Daten des HTTP-Requests an: IP-Adresse, Zeit des Zugriffs und andere Angaben.

Bei einer Registrierung für Chats u.a. oder dem Beitritt zu einem Forum gilt grundsätzlich: Es sollen nur so viele personenbezogene Daten des Nutzers wie unbedingt nötig abgefragt werden und diese Daten dürfen nur für den konkreten Zweck (Zugang zum Forum usw.) gespeichert und genutzt werden. Eine Double-Opt-In-Lösung zur Nutzerregistrierung ist empfehlenswert. Bei der Registrierung sollte zudem vorgesehen sein, dass sich der Nutzer einen Nickname wählen kann, damit so auf die Veröffentlichung des Klarnamens verzichtet werden kann.

Es ist nützlich, bei der Einwilligungserklärung die wichtigsten Informationen kompakt zusammenzufassen. Die Details können dann mit einem weiteren Klick - z.B. in der allgemeinen Datenschutzerklärung - verfügbar gemacht werden. Auch auf die Nutzungsbedingungen (s.u.) kann verlinkt werden.

Die Nutzer sind berechtigt, ihre Einwilligung zur Speicherung der Daten jederzeit schriftlich mit Wirkung für die Zukunft zu widerrufen. In einem solchen Fall ist der entsprechende Zugang zu löschen.

× Nutzungsbedingungen und Netiquetten

Die Rundfunkanstalten haben in Nutzungsbedingungen und Netiquetten die Rahmenbedingungen festzulegen, die von Nutzern vor ihrer Teilnahme an Chats, Foren u.ä. zu akzeptieren sind. Dort soll u.a. auch definiert sein, welche Form der Kommunikation erwünscht ist, was verboten ist und wie bei Verstößen vorzugehen ist.

Beispiele hierfür sind:

» „Netiquette" auf ARD.de:
http://www.ard.de/home/ard/ARD_de_Netiquette/119854/index.html

» Nutzungsbedingungen für die Community bei DasErste.de:
http://www.daserste.de/specials/service/nutzungsbedingungen100.html

» Richtlinien auf tagesschau.de:
https://meta.tagesschau.de/richtlinien

Die Netiquette bzw. die Nutzungsbedingungen sollten – wie die Einwilligung auch - durch den Nutzer aktiv bestätigt werden (z.B. via Checkbox). Die Nutzungsbedingungen können

einen eigenen Passus zum Datenschutz enthalten oder es kann auf die allgemeine Datenschutzerklärung des Onlineangebotes verlinkt werden.

× Löschung von persönlichen Nutzerdaten - Löschung von Inhalten

Persönliche Daten der Nutzer sind zu löschen, sobald sie nicht mehr erforderlich sind. Dies ist der Fall bei Abmeldung des Nutzers oder bei Widerruf der Einwilligung zur Speicherung der Daten. Dem Nutzer sollte zudem selbst die Möglichkeit eingeräumt werden, seinen Account zu löschen (seine Kommentare können dann neutral „Gast" zugewiesen werden)

Wenn die Inhalte der Kommentare nicht den Vorgaben der Netiquette und der Nutzungsbedingungen entsprechen, können sie gelöscht und/oder der Nutzer gesperrt werden. Dies ist u.a. dann von Bedeutung, wenn Dritte durch die Veröffentlichung in ihrem Recht auf informationelle Selbstbestimmung verletzt sind.

× Auf Datensicherheit achten

Aus dem Prinzip der Datensicherheit folgt, dass man geeignete Sicherheitsmaßnahmen natürlich insbesondere für die Passwörter vorsieht. Aber auch die anderen Daten sind fachgerecht vor unbefugten Zugriffen zu sichern.

× Achtung bei der Verwendung von Nutzernamen

Die in den Chats, Foren u.ä. genutzten Namen sind nicht immer die Klarnamen der tatsächlich handelnden Nutzer. Hier können falsche Eindrücke entstehen, wenn Personen bestimmte Äußerungen zugeschrieben werden, ohne dass sie tatsächlich die Quelle sind. Es sollte nicht vorschnell geurteilt, sondern auch hier gewissenhaft recherchiert werden.

× Achtung bei Angeboten für Minderjährige

Bei Angeboten für Minderjährige sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

× Auf sonstige rechtliche Aspekte achten

Bei von Nutzern eingestellten Inhalten (Kommentare, User Generated Content) sind regelmäßig weitere rechtliche Aspekte zu beachten (z.B. Urheberrecht, Persönlichkeitsrecht). Hierzu ist Rücksprache mit dem zuständigen Justitiariat zu halten.

COOKIES

Fast alle Webseiten speichern Cookies auf Geräten (PC, Handy, etc.) eines Benutzers, um eine optimale Kommunikation zwischen der Website und dem Browser des Benutzers sicherzustellen. Cookies sind kleine Textdateien, die lokal im temporären Speicher des Internet-Browsers eines Seitenbesuchers gespeichert werden. Sie sind dazu da, den Nutzer wiederzuerkennen und ihm das Surfen auf einer Webseite zu erleichtern, etwa dadurch, dass der Nutzer seine Zugangsdaten nicht bei jedem Besuch neu eingeben muss. Cookies ermöglichen es aber auch, ein komplexes Nutzungs- und Surfverhalten zu ermitteln.

Es gibt unterschiedliche Arten von Cookies: Cookies können nach ihrer Lebensdauer unterschieden werden - Session Cookie oder permanente Cookie - und danach, zu welchem Anbieter sie gehören - dem Anbieter der Webseite selbst oder einem Drittanbieter, der mit der Webseite verbunden ist.

» Session Cookies (temporäre Cookies)

Sie werden eingesetzt, um einen Benutzer wiederzuerkennen, der auf dieser Webseite gesurft ist oder um zu erkennen, ob ein Benutzer bereits eingeloggt ist. Sitzungscookies werden automatisch gelöscht, wenn der Benutzer den Browser schließt.

» Permanente Cookies (dauerhaft gespeicherte Cookies)

Diese werden auf dem Computer eines Benutzers gespeichert und laufen entweder zu einem bestimmten Datum/innerhalb eines vorgegebenen Zeitrahmens ab oder haben überhaupt kein Ablaufdatum.

Was sagt der Datenschutz?

Cookies sind datenschutzrechtlich relevant, wenn sie über enthaltene Informationen wie etwa Benutzernamen oder IP-Adresse einen Personenbezug herstellen.

× Unproblematisch: Für die Nutzung einer Seite unbedingt erforderliche Cookies

Cookies, die für die aktuelle Nutzung der Seite zwingend erforderlich sind, weil ohne sie ein Onlinedienst technisch gar nicht funktionieren würde, sind datenschutzrechtlich unproblematisch. Dazu gehören z.B. Cookies, die mehrseitige Formulare speichern. Auch geht es hier um Informationen über die Spracheinstellungen oder um Login-Daten für die jeweilige Sitzung (Cookies zur Verbesserung der Funktionalität oder der Leistung/Performance der Webseite).

Regelmäßig handelt es sich hierbei um temporäre Cookies, die nach der Nutzung wieder gelöscht werden.

× Achtung bei optionalen Cookies für zusätzliche Zwecke

Bei optionalen Cookies für zusätzliche Zwecke ist die Rechtslage unklar und umstritten. Das trifft insbesondere zu auf Analyse- und Tracking-Cookies, die die Verfolgung des Nutzerverhaltens im Internet ermöglichen. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann z.B. auf sie zugeschnittene Werbung anzuzeigen. Ebenso betrifft dies Cookies von Social-Media-Plattformen wie Facebook.

Das deutsche Recht kennt aktuell keine direkte Pflicht, die Nutzer in die Verwendung von Cookies einwilligen zu lassen. Danach ist es ausreichend, den Nutzer über den Einsatz dieser optionalen Cookies in der Datenschutzerklärung zu unterrichten und auf ein Widerspruchsrecht hinzuweisen (sog. „Opt-out"-Verfahren). Die einschlägigen europäischen Regelungen fordern dagegen grundsätzlich die aktive Einwilligung des Nutzers nach vorher erfolgter umfangreicher Aufklärung (sog. „Opt-in"-Verfahren).

Checkliste

× Praxis: Informationen in der Datenschutzerklärung und „Opt-out"-Verfahren

Angesichts der unklaren Rechtslage besteht derzeit eine Option darin, bis auf weiteres das „Opt-out"-Verfahren zu praktizieren und abzuwarten, wie sich die deutsche Rechtslage hier möglicherweise ändert. In diesem Fall hat die Rundfunkanstalt über den Einsatz von Cookies umfassend in der Datenschutzerklärung zu informieren und den Nutzer auf sein Widerspruchsrecht beim Einsatz von Cookies und bei der Bildung von Nutzungsprofilen hinzuweisen. Zudem ist dem Nutzer zu erklären, wie er das Setzen von Cookies verhindern bzw. diese durch Einstellungen in seinem Browser löschen kann.

Bei Webanalyse-Tools sollte dem Nutzer auch unmittelbar eine technische Möglichkeit zum Widerspruch eingeräumt werden. In der Regel kann durch Anklicken eines entsprechenden Links das jeweilige Cookie deaktiviert werden (siehe hierzu die Hinweise zur ***Web-Analyse***).

× Rechtlich sicherste Variante: Informationen auf Startseite und „Opt-in"-Verfahren

Angesichts der unklaren rechtlichen Situation ist die sicherste Variante, wenn die Rundfunkanstalt die vorherige Einwilligung des Nutzers einholt. Es sind hierzu sichtbare Informationen auf der Startseite zu hinterlegen, denen der Nutzer wissentlich und aktiv zustimmen kann, und zwar dies bevor das erste Cookie auf dessen Endgerät gelangt. Der Einwilligungstext sollte beim ersten Aufruf der Seite eingeblendet werden. Der Text sollte so konkret wie möglich sagen, um welche Daten es geht, wozu diese genutzt werden und an wen diese Daten weiter gegeben werden. Der Nutzer muss diesen Text mit einem Klick bestätigen. Diese Einwilligung

ist zu protokollieren und vorzuhalten im Falle von Nachfragen.

Wichtig: Ein Pop-up-Fenster ist ungenügend, weil dieses unter Umständen nutzerseitig geblockt werden könnte. Daher greifen fast alle Seitenbetreiber zu sog. Lay-Over-Ein-blendungen am oberen oder unteren Rand des Bildschirms.

Die angezeigten Informationen müssen einen kurzen allgemeinen Hinweis über Cookies und einen Link zu detaillierteren Informationen (in der Regel zur Datenschutzerklärung, alternativ zu einer eigenen Cookie-Informationsseite) enthalten. Zudem muss ein klickbarer Button zur Einwilligung vorhanden sein. Hierbei darf es sich nicht um einen voreingestellten Zustimmungsbutton („gesetztes Häkchen") handeln - dem Nutzer muss die Wahl zwischen Zustimmung und Ablehnung gegeben werden. Und: Eine Ablehnung eines solchen optionalen Cookie darf die Nutzung der Seite nicht beeinträchtigen.

Im Fall einer Nutzerbeschwerde ist der Seitenbetreiber in der Beweispflicht - er muss beweisen, dass der entsprechende Nutzer seine Einwilligung in die Verwendung von Cookies gegeben hat. Allgemeine Texte wie „Durch die weitere Nutzung dieser Webseite erklären Sie sich mit der Verwendung von Cookies einverstanden" sind rechtlich nicht sicher.

Die EU-Kommission bietet für Webseitenanbieter ein Tool - ein sog. Cookie Consent Kit - zur rechtskonformen Umsetzung für den Einsatz von Cookies an (siehe hierzu unter: ***http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm***).

× In jedem Fall: Information zum Einsatz von Cookies in der Datenschutzerklärung!

Wichtig. In allen Varianten hat die Rundfunkanstalt in der Datenschutzerklärung einen entsprechenden Passus zu Cookies und Hinweise für den Nutzer aufzunehmen, wie er das Setzen von Cookies verhindern kann. Es muss eindeutig, leicht auffindbar und in verständlicher Sprache aufgeführt werden,

» was genau in den Cookies gespeichert wird; dabei ist je nach Cookie zu differenzieren,

» zu welchem Zweck gespeichert wird,

» wie lange gespeichert wird,

» wer genau für die Speicherung verantwortlich ist sowie

» dass und wie der Nutzer von seinem Widerrufsrecht Gebrauch machen kann.

× Achtung bei Angeboten für Minderjährige

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

DATENSCHUTZERKLÄRUNG

Webseiten und Apps sammeln inzwischen eine Vielzahl an Daten über ihre Nutzer, die dem Datenschutz unterliegen. Eine Datenschutzerklärung eines Onlineangebots oder einer App ist daher unerlässlich, um die Datensouveränität der Nutzer zu wahren und Vertrauen zwischen Rundfunkanstalt und Nutzer zu schaffen. Sie sollen dem Besucher einer Webseite transparent und verständlich aufzeigen, was häufig von ihm unbemerkt und im Hintergrund mit seinen persönlichen Daten passiert.

Was sagt der Datenschutz?

Das Datenschutzrecht verpflichtet die Rundfunkanstalten, die Nutzer ihres Onlineangebotes über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über eine etwaige Weitergabe der Daten an Dritte allgemein in einer leicht verständlichen, lesbaren Weise zu informieren.

Eine Datenschutzerklärung ist strikt zu unterscheiden

» von einer datenschutzrechtlichen Einwilligung:

In der Datenschutzerklärung erläutert die Rundfunkanstalt rein informierend, was sie mit den Daten (aufgrund gesetzlicher Befugnisse) unternimmt. Bei einer datenschutzrechtlich relevanten Einwilligung holt die Rundfunkanstalt eine explizite Zustimmung des Nutzers ein, um die Daten in einer Art und Weise zu nutzen, die das Gesetz nicht per se erlaubt.

» vom Impressum einer Webseite:

Ein Impressum - manchmal auch „Anbieterkennzeichnung" genannt - ist i.d.R. gesetzlich erforderlich für Veranstalter einer Webseite. Dabei handelt es sich um eine allgemeine medienrechtliche Pflicht: Besucher einer Webseite sollen wissen können, mit wem sie es zu tun haben. Das dient allerdings auch dem datenschutzrechtlichen Prinzip der Transparenz. Der Link oder Reiter auf das Impressum sollte als solcher benannt werden. Von jeder Unterseite aus sollte der Nutzer mit einem Klick herausfinden können, wer Veranstalter des Angebots ist.

Checkliste

× Form: Allgemein verständlich, leicht auffindbar und jederzeit abrufbar

Die Datenschutzerklärung sollte in allgemein verständlicher, lesbarer Form formuliert sein. Technische oder juristische Fachbegriffe und Formulierungen sind daher zu vermeiden.

Bereits auf der Startseite muss ein eindeutiger, leicht auffindbarer Hinweis auf diese Informationen zu finden sein. Zudem müssen sie jederzeit abrufbar sein. Die Datenschutzerklärung sollte daher auf der Internetseite unter einem eigenen Menüpunkt „Datenschutzerklärung" oder „Datenschutzhinweis" als Link eingebunden und von jeder Seite und Unterseite aus erreichbar sein. Bei Änderungen ist der Inhalt zu aktualisieren.

Bei Telemedienangeboten für Minderjährige ist zusätzlich eine verständliche Form für Kinder und Jugendliche erforderlich (siehe hierzu die Hinweise zum ***Minderjährigen-Datenschutz***).

× Inhalt: Was muss alles drin sein?

Eine Datenschutzerklärung muss grundsätzlich für das gesamte Onlineangebot formuliert werden. Die Angaben, die zu machen sind, richten sich nach den spezifischen Angeboten und Funktionen der Seite.

Grundsätzlich gilt es, die Nutzer der Seite über die Art, den Umfang und die Zwecke der Erhebung und die Verwendung personenbezogener Daten zu unterrichten. Je mehr Daten von den Nutzern erhoben werden und je sensibler die Daten sind, desto ausführlicher muss die Unterrichtung sein. Ebenfalls zu benennen sind eventuelle Weitergaben der Daten in Länder außerhalb der EU.

Informationen darüber, welche personenbezogenen Daten des Nutzers erfasst werden

» Bei Aufruf und Nutzung der Seite oder App

Server-Log-Daten (Datum und Uhrzeit des Besuches, die verwendete IP-Adresse, Browsertyp/-version und Betriebssystem; besuchte Webseiten und Herkunftsseite); Gerätedaten; Standortdaten o.ä.

» Aufgrund der Anmeldung (Registrierung)

Name; Geschlecht; Geburtsdatum; Anschrift; Kontaktdaten (Mail, Telefonnummern), Fotos, Standortdaten o.ä.

» **Aufgrund sonstiger Funktionen, insb. Anwendungen von externen Diensteanbietern**

Gewinnspiele; Nutzerforen; Kommentarfunktionen; Newsletter-Abonnements; Kontaktformulare; Webanalysen; Social-Media-Funktionen; Tools von sonstigen externen Diensten und Drittplattformen o.ä.

Informationen darüber, auf welche Weise und für welchen Zweck die Daten erhoben und genutzt werden

» **Cookies und Plugins**

Welche Cookies oder Plugins werden genutzt, welche Daten werden dabei wozu durch die Rundfunkanstalt oder Dritte genutzt?

» **Tracking-Tools**

Welche Tracking-Dienste werden eingesetzt, welche Tracking-Daten werden wozu genutzt?

» **Zugriffsrechte (bei Apps)**

Auf welche Daten wird zugegriffen? Weshalb erfolgt wann wozu ein Zugriff?

» **Eingaben des Nutzers**

Welche Daten stammen für welchen Zweck von Eingaben des Nutzers selbst?

» **Einwilligung**

Es ist transparent zu machen, welche Datenerhebungen und -verarbeitungen zu welchem Zweck von der Einwilligung des Nutzers abhängen.

Information über Nutzerrechte

» **Widerruf der Einwilligung**

Der Nutzer ist auf die Möglichkeit des Widerrufs einer erteilten Einwilligung hinzuweisen, inklusive einer einfachen Kontaktmöglichkeit (z.B. per E-Mail).

» **Anonyme/pseudonyme Nutzung**

Der Nutzer ist über die Möglichkeit zu informieren, das Onlineangebot anonym oder unter Pseudonym nutzen zu können.

» **Widerspruchsrecht bei Cookies, pseudonymen Nutzungsprofilen**

Der Nutzer ist auf sein Widerspruchsrecht beim Einsatz von Cookies und bei der Bildung von Nutzungsprofilen hinzuweisen (siehe die Hinweise zur ***Web-Analyse***).

× Nennung eines Ansprechpartners

Am Ende der Datenschutzerklärung sollte ein Ansprechpartner für datenschutzrechtliche Anfragen und Beschwerden genannt werden (z.B. der anstaltseigene Datenschutzbeauftragte). Dabei sollte eine einfache Möglichkeit der Kontaktaufnahme (z.B. via E-Mail und Telefon) angeboten werden.

× Hinweis auf Drittplattformen, auf denen die Rundfunkanstalt präsent ist

Aus Gründen der Transparenz sollte die Rundfunkanstalt in ihrer Datenschutzklärung auch informieren, dass sie mit eigenen Auftritten auf Social-Media-Plattformen und anderen Drittplattformen präsent ist. Dem Nutzer sollte erklärt werden, welche Datenschutzrichtlinie für die Nutzung der jeweiligen Drittplattformen gilt (verbunden mit der Bitte an den Nutzer, diese aufmerksam zu lesen).

DRITTPLATTFORMEN

Die Rundfunkanstalten sind mit ihren Angeboten und Inhalten auf verschiedenen Drittplattformen präsent. Neben den Social-Media-Plattformen wie Facebook, Twitter und Google+ sind die Anstalten z.B. auf der Videoplattform YouTube, auf Foto-/Content-Plattformen wie Instagram und Pinterest oder Streamingdiensten wie Spotify vertreten. Daneben gibt es noch eine Vielzahl von anderen Drittplattformen, die von den Rundfunkanstalten im Hinblick auf ihre publizistische Bedeutung getestet oder zeitweise genutzt werden.

Was sagt der Datenschutz?

Drittplattformen - insbesondere soziale Netzwerke wie Facebook u.a. - sind aus datenschutzrechtlicher Sicht sehr problematisch. Es ist davon auszugehen, dass diese Plattformen aus verschiedenen Gründen regelmäßig nicht den deutschen Datenschutzstandards entsprechen. Bedenken bestehen insbesondere in Bezug auf die Anforderungen an Transparenz, Datensparsamkeit und wirksame Einwilligung. Die meisten Drittplattformanbieter speichern die Daten zudem häufig außerhalb der EU in Ländern wie den USA, die kein vergleichbares Niveau an Datenschutz gewährleisten.

Aber: Im Hinblick auf die Präsenz von Rundfunkanstalten auf Drittplattformen ist grundsätzlich davon auszugehen, dass der jeweilige Plattformanbieter datenschutzrechtlich verantwortlich bleibt. Eine eigene datenschutzrechtliche Verantwortlichkeit trifft die Rundfunkanstalten bei der Nutzung dieser Plattformen nach geltendem Recht nicht.

Unabhängig von der formalrechtlichen Verantwortlichkeit sollte die Rundfunkanstalt ihre Präsenz auf Drittplattformen so datenschutzgerecht wie möglich ausgestalten.

Checkliste

× Überprüfung der Datenschutzrichtlinien / AGB der Drittplattform - Check des publizistischen Mehrwerts

Sofern die Rundfunkanstalt auf einer Drittplattform präsent sein will, sollten vorab die Datenschutzrichtlinien sowie die sonstigen AGB oder Nutzungsbedingungen des Drittanbieters

geprüft werden. Oftmals enthalten diese AGB für die Rundfunkanstalt problematische urheberrechtliche und sonstige Klauseln. Möglicherweise lässt sich der jeweilige Anbieter im Rahmen einer eigenen Vereinbarung mit allen Rundfunkanstalten zur Einhaltung der deutschen Standards bewegen.

Regelmäßig weisen Drittplattformen die bekannten Datenschutzmängel auf, die die Nutzer dieser Angebote treffen können. Insofern sollte gewissenhaft abgewogen werden, ob der publizistische Mehrwert trotzdem für die Präsenz der Rundfunkanstalt auf dieser Plattform spricht. Dieser Check sollte regelmäßig wiederholt werden.

× Datenschutzkonformes Verhalten der Rundfunkanstalt auf Drittplattformen

Unabhängig von der formalrechtlichen Verantwortlichkeit sollte die Rundfunkanstalt ihre Präsenz auf Drittplattformen so datenschutzgerecht wie möglich ausgestalten.

Dies bedeutet z.B., dass die Rundfunkanstalt die Nutzer nicht dazu einladen darf, sensible Informationen (z.B. im Rahmen von Upload-Aktionen) preiszugeben.

Auch Datenflüsse zwischen Drittplattform und Rundfunkanstalt ohne Wissen und Wollen des Nutzers sind zu verhindern (siehe hierzu auch die Hinweise zum ***Embedding von fremden Inhalten***).

Machen Nutzer von ihren Rechten (Recht auf Auskunft, Berichtigung oder Löschung) Gebrauch, sollte die Rundfunkanstalt - soweit technisch möglich und vom Aufwand her zumutbar - diese Daten selbst löschen bzw. sperren. Eine Verweisung des Nutzers an den Plattformbetreiber sollte erst im zweiten Schritt für die Maßnahmen erfolgen, die nur durch den Plattformanbieter selbst zu realisieren sind.

× Hinweis auf Nutzungsbedingungen der Drittplattform

Aus Gründen der Nutzerfreundlichkeit sollte die Rundfunkanstalt in ihrer Datenschutzerklärung transparent aufzeigen, dass sie mit eigenen Seiten/Kanälen und Inhalten auf Social-Media-Plattformen und anderen Drittplattformen präsent ist.

Dem Nutzer sollte erklärt werden, dass die Datenverarbeitung durch die Betreiber der Drittplattformen außerhalb der Verantwortung der Rundfunkanstalten liegt. In diesem Kontext sollte - z.B. per Link - auch auf die allgemeinen Geschäftsbedingungen bzw. Datenschutzrichtlinien der jeweiligen Drittplattformen verwiesen werden.

Es bietet sich hier an, bei den Drittplattformen genau zu differenzieren und für jeden Drittanbieter jeweils einen eigenen Passus in die Datenschutzerklärung aufzunehmen.

EMBEDDING VON FREMDEN INHALTEN: PLUGINS, VIDEOS & CO

Embedding bedeutet das Einbinden fremder Inhalte auf den eigenen Webseiten oder Apps. Eingebettet werden z.B. Fotos, Grafiken, Audio- und Videofiles, Textnachrichten sowie Social-Media-Plugins zum Teilen, ‚Liken' u.a. von Inhalten.

Das Einbinden fremder Inhalte wird dabei häufig über sog. iFrames (Inlineframes) realisiert. Einfach gesprochen ist der iFrame auf einer bestimmten Webseite wie ein kleines Fenster, in dem eine ganz andere Webseite, die auf einem anderen Server liegt, angezeigt wird. Der Nutzer schaut dann eigentlich gerade mehrere Webseiten parallel an. Dank Embedding muss der Nutzer also z.B. keinen eigenen Video-Player implementieren oder die Video-Dateien selbst hosten.

Was sagt der Datenschutz?

Beim Embedding externer Inhalte in die rundfunkeigenen Onlineseiten oder Apps können die Anbieter dieser Inhalte (nachfolgend bezeichnet als „Drittanbieter") auf Daten der Nutzer der Webseite der Rundfunkanstalt zugreifen und für sich nutzen.

Sobald der Nutzer eine Seite der Rundfunkanstalt mit eingebetteten Inhalten aufruft, wird - sofern die Rundfunkanstalt keine besonderen Vorkehrungen trifft - regelmäßig die IP-Adresse der Nutzer ohne Vorwarnung, ohne Wissen und möglicherweise gegen seinen Willen an die Drittanbieter übertragen, ohne dass der Nutzer dieses Angebot angeklickt hat. Durch den Einsatz von Cookies erfassen die Drittanbieter von Social-Media-Funktionen zudem das individuelle Surfverhalten der Nutzer. Für ein solches User-Tracking ist es noch nicht einmal erforderlich, dass der Nutzer beim jeweiligen sozialen Netzwerk eingeloggt oder dort Mitglied ist. Diese Übertragung von Nutzerdaten an Drittanbieter ist aber nur mit Einwilligung des Nutzers zulässig.

Erfolgt die Datenverarbeitung durch den Drittanbieter auf der Grundlage einer entsprechenden Vereinbarung im Auftrag der Rundfunkanstalt, so wie bei Blog- bzw. Kuratiertools (z.B. Scribble Live) und Tools von Kartenanbietern (z.B. Bing-Maps), wird die Datenverarbeitung durch den Drittanbieter der Rundfunkanstalt zugerechnet. In diesem Fall ist keine Einwilligung des Nutzers erforderlich.

Checkliste

× Einbettung aus redaktionellen Gründen erforderlich?

Beim Einbetten von externen Inhalten sollte der redaktionelle Mehrwert der Verwendung der Inhalte gegen die datenschutzrechtlichen Risiken im Einzelfall abgewogen werden. Bei der Abwägung sind die jeweiligen Datenschutzrichtlinien des Drittanbieters zu berücksichtigen.

× Gibt es datenschutzfreundliche Voreinstellungen?

Vor dem Embedding von externen Inhalten sollte geprüft werden, ob beim Drittanbieter datenschutzfreundliche Voreinstellungen bestehen.

Einzelne Anbieter wie z.B. YouTube scheinen inzwischen die Möglichkeit zu bieten, Inhalte so einzubetten, dass Cookies nicht zur Profilbildung genutzt werden. Dazu muss ein erweiterter Datenschutzmodus aktiviert werden. YouTube erklärt den erweiterten Datenschutzmodus wie folgt: „Wenn du diese Option aktivierst, werden von YouTube keine Informationen über die Besucher auf deiner Website gespeichert, es sei denn, Sie sehen sich das Video an". Zumindest vor dem Klick auf das Video scheint dann kein Tracking stattzufinden. Eine wirkliche Kontrolle, was die Einbettung tatsächlich auslöst, gibt es nicht. Überdies ist auch bei Verwendung des erweiterten Datenschutzmodus die Information des Nutzers über die Datenverarbeitung durch den Drittanbieter nach dem Klick erforderlich.

× Einsatz der (modifizierten) Zwei-Klick-Lösung

Für ein datenschutzkonformes Embedding von Plugins und anderen Inhalten von Drittanbietern sollte die von heise.de entwickelte sog. „Zwei-Klick-Lösung" – zumindest in einer modifizierten Version - eingesetzt werden.

Die Zwei-Klick-Lösung ist derzeit weit verbreiteter Standard in den Onlineangeboten der Rundfunkanstalten: Dabei sind die Plugins bei Aufruf der Onlineseite der Rundfunkanstalt inaktiv – es fließen keine Daten an den Drittanbieter. Erst nach der Aktivierung einer Zwischenschaltfläche (Grafik) durch den Nutzer beginnt die Datenübertragung. Der Nutzer wird, sobald er über die Schaltfläche mit dem Mauszeiger fährt, über die Datenweitergabe informiert. Bei Touch-Geräten erfolgt die Information über die Datenweitergabe nach dem ersten Klick.

Allerdings ist dieses Vorgehen nicht sehr nutzerfreundlich und behindert gerade bei Social Plugins die programmlichen Interessen von Fangewinnung und Reichweitensteigerung. Der Nutzer muss für den Besuch einer einzigen Webseite einschließlich der eingebetteten Inhalte zahlreiche Klicks durchführen und Warnhinweise zur Kenntnis nehmen.

Die Zwei-Klick-Lösung kann auch in einer modifizierten, nutzerfreundlicheren Version eingesetzt werden: Dabei wird der Nutzer pro Session beim Anklicken des ersten eingebetteten Inhalts auf einer Webseite auf einer Zwischenseite über die Datenverarbeitung durch die Drittanbieter aufgeklärt und hat die Wahl, auf weitere entsprechende Hinweise auf der Webseite

zu verzichten. Wenn er darauf verzichtet, wird die Zwischenseite bei nachfolgenden Einbettungen nicht jedes Mal wieder eingesetzt. Er hat damit die Option zur „generellen" Freischaltung aller Drittanbieter-Inhalte auf der jeweiligen Webseite. Dieses Verfahren muss die Möglichkeit vorsehen, die pauschal erklärte Zustimmung jederzeit zu widerrufen.

× Shariff-Button für Social-Media-Plugins

Für Social Plugins von Facebook, Twitter und Google+ hat heise.de eine neue, verbesserte Lösung entwickelt, den sog. Shariff-Button.

Auch mittels Shariff werden zunächst keine Daten übertragen. Die Nutzer können die jeweilige Webseite besuchen, ohne dass gleichzeitig ihr Surfverhalten für die sozialen Netzwerke sichtbar wird, denn die Daten des Nutzers werden auf einem Zwischenserver gespeichert, so dass sie von den sozialen Netzwerken nicht direkt „abgefangen" werden. Der Shariff-Button stellt die Verbindung zum sozialen Netzwerk erst dann her, wenn der Nutzer aktiv wird und auf den Button klickt. Der Vorteil von Shariff ist, dass es nur einen Button gibt und dieser farbig gestaltet werden kann, so dass er im Zweifel von den Original-Plugins zu unterscheiden ist.

Man benötigt also nur einen Klick für ein „Like" oder „Share". Der erste Klick, mit dem die Buttons bisher bei der Zwei-Klick-Lösung aktiviert werden mussten, ist obsolet geworden.

× Information über das Embedding von Inhalten und Tools von Drittanbietern in der Datenschutzerklärung

In der Datenschutzerklärung sollte die Rundfunkanstalt umfassend über das Einbinden von externen Inhalten und Social Plugins auf ihren Seiten informieren. Die Hinweise sollten nach Drittanbietern differenziert werden. Dabei sollten auch auf die Zwei-Klick-Lösung sowie die Shariff-Lösung Bezug genommen und die Funktionsweise erläutert werden.

Über den Einsatz von Blog-/Kuratiertools und sonstigen Tools Dritter, die die Rundfunkanstalt auf der Grundlage einer entsprechenden Vereinbarung auf ihren Seiten einsetzt, sollte im Sinne größtmöglicher Transparenz ebenfalls informiert werden.

× Achtung Auftragsdatenverarbeitung

Manche externen Tools - wie z.B. Live-Blogging - sind Werkzeuge, die die Rundfunkanstalt zur Erzeugung ihrer eigenen Inhalte und Integration von Social-Media-Kanälen verwendet. In der Regel fließen aber auch hier Daten zum Drittanbieter. Um die interaktiven Features des Live-Blogs nutzen zu können, werden sowohl die IP-Adresse als auch weitere gerätebezogene Informationen an den Dienstleister übertragen. Zudem werden temporäre Cookies auf der Festplatte des Nutzers gesetzt.

Verarbeitet der Anbieter des Tools in diesem Zusammenhang Nutzerdaten, so tut er dies im Auftrag der Rundfunkanstalt; die Datenverarbeitung wird der Rundfunkanstalt zugerechnet. Es gelten hier die Hinweise zur ***Auftragsvergabe an Dritte***. Mit der Vereinbarung muss insbesondere sichergestellt werden, dass die Datenverarbeitung durch den Anbieter nur mit Wissen und Wollen der Nutzer erfolgen.

× Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

GEWINNSPIELE

Gewinnspiele sind als Teil des redaktionellen Angebots auch in den Telemedienangeboten der Rundfunkanstalten möglich. Es gibt Gewinnspiele im rundfunkeigenen Angebot (z.B. über ein Kontaktformular), die in der Regel auch On-Air beworben werden, mit Mitspielmöglichkeiten auf dem eigenen Angebot und/oder auf Drittplattformen. Es gibt aber auch Gewinnspiele, die ausschließlich auf Drittplattformen durchgeführt werden (z.B. „Liken und teilnehmen", „Der User-Kommentar mit den meisten Likes gewinnt").

Was sagt der Datenschutz?

Welche Nutzerdaten wie lange bei einem Online-Gewinnspiel abgefragt und verarbeitet werden können, hängt von der konkreten Ausgestaltung des Spieles ab. Hier gibt es zahlreiche Varianten. Bei allen Varianten ist aber darauf zu achten, dass nur die Nutzerdaten erhoben werden, die für die Durchführung des Gewinnspiels tatsächlich notwendig sind. Die erhobenen Daten dürfen nur zur Durchführung des Gewinnspiels verwendet werden (also nicht z.B. auch zur Zusendung eines Newsletter). Sie dürfen auch nur so lange gespeichert werden, wie es für die Durchführung des Gewinnspiels erforderlich ist. Danach sind die Daten zu löschen.

Checkliste für Gewinnspiele im anstaltseigenen Onlineangebot

× Teilnahmebedingungen mit Informationen zum Datenschutz

Jedes Gewinnspiel braucht Teilnahmebedingungen. Diese sind vorab festzulegen. Darin können auch die nötigen Informationen zum Datenschutz integriert werden. Bei einem Gewinnspiel ist (z.B. auf dem Teilnahmeformular) stets ein Checkbox-Feld vorzusehen, in dem der User aktiv anklicken muss, dass die Teilnahmebedingungen gelesen und akzeptiert wurden.

× Zweckbindung und Datensparsamkeit

Die Rundfunkanstalt darf nur die Daten als Pflichtfelder abfragen, die für die Durchführung des Gewinnspiels erforderlich sind. Die Daten dürfen auch für keine anderen Zwecke verwendet werden.

Die Pflichtfelder sind entsprechend kenntlich zu machen. Beispiele:

» Die Abfrage der Mailadresse ist ausreichend, wenn ein Versand des Preises (z.B. Tickets) online erfolgt und um eine Identifikationsmöglichkeit zu haben (z.B. um eine Mehrfachteilnahme zu verhindern).

» Die (zusätzliche) Telefonnummer ist zulässig, wenn eine telefonische Kontaktaufnahme (Rückruf) notwendig oder ein Telefongespräch on air geplant ist.

» Die Abfrage der Postadresse ist zulässig, wenn der Gewinn verschickt werden muss. Aber: In der Regel ist hier jedoch eine vorherige Kontaktaufnahme per Mail oder Telefon mit den Gewinnern möglich, so dass eine Adressangabe als Pflichtfeld bei allen Teilnehmern nicht immer erforderlich ist. Viele Nutzer sind außerdem nicht bereit, die Adresse als Pflichtfeld anzugeben.

Alle weiteren Angaben dürfen - sofern redaktionell gewünscht - nur als freiwilliges Datum abgefragt werden, immer verbunden mit dem ausführlichen Datenschutzhinweis, zu welchem Zweck diese konkrete Datenverarbeitung erfolgt und dass die Daten nicht an Dritte weitergegeben werden. Ein Verweis auf die „allgemeinen" Datenschutzhinweise der Rundfunkanstalt ist insofern nicht ausreichend. Diese zusätzliche Abfrage sollte nur dann durchgeführt werden, wenn ein echter redaktioneller Mehrwert zu erwarten ist.

Der Nutzer ist darüber zu informieren, dass er bei weiteren freiwilligen Angaben seine Einwilligung widerrufen kann.

× An die Löschung denken

Die Daten der Teilnehmer am Gewinnspiel sind zu löschen, sobald das Gewinnspiel beendet und eine angemessene „Reklamationszeit" abgelaufen ist. Die konkreten Löschfristen hängen auch von der „Größe" des Gewinnspiels ab. Je nach Wertigkeit des Gewinns können die Anforderungen an die Länge der Aufbewahrungsfristen variieren.

Die Daten der Gewinner sind zudem bei anderen Stellen in der Rundfunkanstalt zu Dokumentationszwecken auch nach Ablauf des Gewinnspiels zu speichern (Steuer, Revision usw.) und sind dort nach den jeweiligen internen Regelungen zu löschen.

Außerdem muss sichergestellt sein, dass nach der Speicherfrist tatsächlich die Löschung der Daten erfolgt. Sofern keine entsprechende Programmierung erfolgen kann, muss notfalls auch eine manuelle Löschung erfolgen. Der Aufwand, der dies möglicherweise verursacht, ist kein Grund, einen „Datenfriedhof" vorzuhalten.

× Minderjährigen-Datenschutz

Beim Umgang mit Daten von Minderjährigen sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

× Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur in der Rundfunkanstalt verarbeitet und gespeichert werden. Sofern ein Dienstleister mit der Durchführung und/oder dem Hosting für das Gewinnspiel beauftragt ist, sind die Hinweise zur ***Auftragsvergabe an Dritte*** zu beachten.

× Beachtung der sonstigen Vorgaben für Gewinnspiele

Es sind die sonstigen Vorgaben der öffentlich-rechtlichen Rundfunkanstalten für Gewinnspiele zu beachten (vgl. ARD-Richtlinien für Werbung, Sponsoring, Gewinnspiele und Produktionshilfe vom 12. März 2010, ***http://www.ard.de/download/553234/ARD_Richtlinien_fuer_Werbung__Sponsoring__Gewinnspiele_und_Produktionshilfe_in_der_Fassung_vom_12_3_2010.pdf***).

Checkliste für Gewinnspiele ausschließlich auf Drittplattformen:

× Verantwortlichkeit des Plattformanbieters

Es gelten grundsätzlich die Teilnahmebedingungen und Datenschutzbestimmungen des jeweiligen Plattformanbieters (siehe hierzu die Hinweise zu ***Drittplattformen***).

× Achtung bei Nutzerverarbeitung auch durch die Rundfunkanstalt

Sobald die Nutzerdaten anlässlich des Gewinnspiels aber auch in der Rundfunkanstalt verarbeitet werden, gelten die o.g. Vorgaben.

× Beachtung der sonstigen Vorgaben der Drittplattform

Es sind die sonstigen AGB/Richtlinien der jeweiligen Drittplattform zur Veranstaltung von Gewinnspielen zu beachten (vgl. z.B. Nutzungsbedingungen von Facebook ***www.facebook.com/page_guidelines.php***).

INSTANT MESSAGING

Instant Messaging ist eine sehr verbreitete Kommunikationsmethode, bei der sich mindestens zwei Teilnehmer per Textnachrichten unterhalten. Populäre Instant Messaging-Dienste sind z.B. WhatsApp, Snapchat oder Facebook Messenger.

Dabei löst der Absender die Übermittlung aus (sog. „Push-Verfahren"), so dass die Nachrichten möglichst unmittelbar (englisch „instant") beim Empfänger ankommen. Viele Instant Messenger unterstützen zusätzlich die Übertragung von Dateien und Audio- und Video-Streams. Benutzer können sich gegenseitig in ihrer Kontaktliste führen und sehen dann an der Präsenzinformation, ob der andere zu einem Gespräch bereit ist.

Was sagt der Datenschutz?

Es gibt viele Anbieter auf dem Markt, die jedoch unterschiedlich mit Datenschutz und IT-Sicherheit umgehen. Viele Messenger-Anbieter informieren den Nutzer nicht oder unzureichend über ihre Datenschutzbestimmungen. Viele Messenger-Apps verzichten zudem auf die Verschlüsselung der Kommunikation. So können Inhalte, Kontakte und andere vertrauliche Daten ausgelesen werden. Im privaten Umfeld liegt die Entscheidung zwar beim Nutzer, ob Datenschutz- und IT-Sicherheitsaspekte eine Rolle spielen. Wenn eine Rundfunkanstalt Instant Messaging-Dienste als Kommunikationsmittel nutzt, sollte sie im Rahmen ihrer Möglichkeit auf einen datenschutzkonformen Einsatz achten.

Checkliste

× Datensparsamkeit und Zweckbindung

Es gelten die allgemeinen Grundsätze (vgl. ***Datenschutz „Basics"***):

Es sollen so wenig Daten wie möglich erhoben werden; die Daten dürfen jenseits der journalistisch-redaktionellen Nutzung nur so lange gespeichert werden, wie es für diesen Zweck

erforderlich und notwendig ist. Sie dürfen nicht anderweitig verwendet werden. Danach sind die Daten zu löschen.

Die Rundfunkanstalt hat Nutzungsstatistiken anonym - also ohne Personenbezug - zu führen.

× Information in Datenschutzerklärung

In der allgemeinen Datenschutzerklärung sind die Nutzer über den Einsatz von Instant Messengers durch die Rundfunkanstalt zu informieren.

× An die Löschung denken

Bei allen Kontaktformen muss sich die Redaktion darüber klar sein, wie lange welche Nutzerdaten warum aufbewahrt werden. Dazu muss man trennen, ob die personenbezogenen Daten - z.B. auch die eingesandten Fotos, „Geschichten" usw. - der Nutzer journalistisch-redaktionell genutzt werden (sollen) und eine Archivierung erfolgen soll oder nicht (z.B. bei Gewinnspielen/Kartenverlosungen/Staumeldern usw.).

Es ist sinnvoll, sich generell auf ein Löschkonzept für die Daten, die auf Servern der Rundfunkanstalt liegen, zu verständigen. Außerdem muss sichergestellt werden, dass nach der Speicherfrist auch tatsächlich eine Löschung der Daten erfolgt. Sofern hier keine entsprechende Programmierung erfolgen kann, muss notfalls auch eine händische Löschung erfolgen.

Wenn eine vom Löschkonzept abweichende Speicherung der Nutzerdaten gewünscht ist (z.B. bei „Stammschreibern"), ist eine gesonderte Einwilligung der Betroffenen einzuholen.

Eine Löschung ist nicht erforderlich, wenn die Daten anonymisiert werden.

× Lokale Datenspeicherung – keine automatische Synchronisation mit Dritten

Bei der Auswahl des Dienstes sollte darauf geachtet werden, dass nur eine lokale Speicherung der Daten auf dem Gerät erfolgt und keine automatische Synchronisation mit Drittanbietern erfolgt.

× Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur in der Rundfunkanstalt verarbeitet und gespeichert werden. Sofern ein Dienstleister mit der Durchführung und/oder dem Hosting beauftragt ist, sind die Hinweise zur ***Auftragsvergabe an Dritte*** zu beachten.

× Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

MAILKONTAKT, KONTAKTFORMULAR, NEWSLETTER

Das Internet bietet vielfältige Möglichkeiten der Kontaktaufnahme mit dem Nutzer. Neben dem direkten Mail-Kontakt zwischen Nutzer und Rundfunkanstalt können Online-Kontakt-Formulare eingesetzt werden. Über Newsletter können User gezielt über ausgewählte Themen informiert werden.

Was sagt der Datenschutz?

Beim Kontakt mit Usern gilt bei allen Varianten grundsätzlich folgendes: Es sollen immer nur so viele bzw. wenige personenbezogene Daten wie unbedingt nötig abfragt werden. Die abgefragten Daten dürfen immer nur für einen ganz bestimmten Zweck erfolgen. Danach ist eine - notfalls manuelle - Löschung erforderlich.

Checkliste

× Zweckbindung und Datensparsamkeit

Die Rundfunkanstalt darf nur solche Daten als Pflichtangaben abfragen, die für den konkreten Zweck - Kontaktaufnahme, Zusendung eines Newsletters usw. - unbedingt notwendig sind (kein „nice to have"). Die Pflichtfelder sind entsprechend kenntlich zu machen.

Sofern in einem Kontaktformular weitere persönliche Daten abgefragt werden, ist darauf hinzuweisen, dass dies keine Pflichtangaben, sondern freiwillige Angaben sind. Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es erforderlich ist und für keine anderen Zwecke verwendet werden.

× Besonderheiten beim Newsletter

Der Nutzer muss den Newsletter ausdrücklich bestellen, d.h.: Newsletter dürfen nie unverlangt zugesandt werden. Neben dem Bestellformular ist auch bereits die Möglichkeit zur Abbestellung des Newsletters bereitzustellen.

» Zur rechtssicheren Erklärung der Einwilligung ist das „Double-Opt-in"-Verfahren einzusetzen: Der Interessent erhält nach der Anmeldung eine Begrüßungsnachricht, darin wird er aufgefordert einen Link anzuklicken. Erst danach darf seine E-Mail-Adresse für den Empfang des Newsletters aktiviert werden. Damit kann verhindert werden, dass jemand eine fremde Mail-Adresse verwendet. Der gesamte Vorgang ist zu dokumentieren.

» In jedem Newsletter muss der Nutzer deutlich sichtbar darauf hingewiesen werden, dass er den Newsletter jederzeit abbestellen kann. Hierzu ist ein Link in die Newsletter-Mail zu setzen.

» Wie immer gilt die Zweckbindung: Daten eines Nutzers, die der Rundfunkanstalt z.B. im Rahmen der Bestellung eines Newsletters übermittelt wurden, dürfen auch nur für diesen Newsletter und nur solange genutzt werden, wie das Abo läuft. Sobald der Nutzer den Newsletter wieder abbestellt, sind seine Daten zu löschen bzw. zu anonymisieren.

× Informationen in der Datenschutzerklärung

In der allgemeinen Datenschutzerklärung sind die Nutzer über die Möglichkeiten der Kontaktaufnahme zu informieren.

× An die Löschung denken

Bei allen Kontaktformen muss sich die Redaktion darüber klar sein, wie lange welche Nutzerdaten warum aufbewahrt werden. Dazu muss man trennen, ob die personenbezogenen Daten - z.B. auch die eingesandten Fotos, „Geschichten" usw. - der Nutzer journalistisch-redaktionell genutzt werden (sollen) und eine Archivierung erfolgen soll oder nicht. Statistiken über Nutzer können anonym geführt werden.

Es ist sinnvoll, sich generell auf ein Löschkonzept zu verständigen. Außerdem muss sichergestellt werden, dass nach der Speicherfrist auch tatsächlich eine Löschung der Daten erfolgt. Sofern keine entsprechende Programmierung erfolgen kann, muss notfalls eine händische Löschung erfolgen.

Wenn eine vom Löschkonzept abweichende Speicherung der Nutzerdaten gewünscht ist (z.B. bei „Stammschreibern"), ist eine gesonderte Einwilligung der Betroffenen einzuholen.

× Datensicherheit - verschlüsselte Übertragung

Die Kommunikation mit Nutzern über das Internet ist so sicher wie möglich zu gestalten, sobald persönliche Daten übertragen werden. Insofern sollte stets eine verschlüsselte Übertragung ermöglicht werden, sofern dies technisch realisierbar und vom Aufwand her verhältnismäßig

ist.

Bei Kontaktformularen im eigenen Angebot sollte eine Verschlüsselung über ein anerkanntes, dem Stand der Technik entsprechendes Verschlüsselungsverfahren zur sicheren Übertragung von Informationen angeboten werden.

Auch bei Mail-Kontakt ist - sofern machbar - eine End-to-End-Verschlüsselung zu empfehlen. Auch wenn dieses Verfahren aufwändig ist, sollte eine End-to-End-Verschlüsselung jedenfalls dann eingesetzt werden, wenn ein Kontakt im Zusammenhang mit journalistischer Recherche be- bzw. entsteht.

× Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

× Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur in der Rundfunkanstalt verarbeitet werden. Sofern ein Dienstleister für den konkreten Kontakt mit dem Nutzer mit der Durchführung und/oder dem Hosting beauftragt ist, sind die Hinweise zur ***Auftragsvergabe an Dritte*** zu beachten.

MINDERJÄHRIGEN-DATENSCHUTZ

Die Rundfunkanstalten wenden sich mit ihren Telemedienangeboten auch an Kinder und Jugendliche. Beispiele für Angebote, bei denen personenbezogene Daten von Minderjährigen erhoben werden, sind Newsletter, Gästebücher und Chats, Gewinnspiele und Mitmachaktionen, die eine aktive Eingabe von Daten erfordern. Beim Umgang mit personenbezogenen Daten von Minderjährigen gelten besondere Anforderungen.

Was sagt der Datenschutz?

Die Nutzung von Angeboten durch Kinder und Jugendliche ist unproblematisch, wenn keine personenbezogenen Daten des Kindes bzw. Jugendlichen explizit abgefragt werden. Die beim Besuch einer Seite ohnehin anfallende IP-Adresse ist notwendig zur Bereitstellung des Dienstes und wäre insoweit unkritisch.

Komplizierter wird es, wenn persönliche Daten der jungen Nutzer wie z.B. Name oder E-Mail-Adresse abgefragt werden. Dies ist grundsätzlich nur mit Einwilligung des Kindes bzw. des Jugendlichen zulässig. Kinder und Jugendliche können in die Verarbeitung ihrer Daten allerdings nur wirksam einwilligen, sofern sie verstehen, welche Konsequenzen dies für sie haben kann, wenn ihre Daten von einem Internet-Unternehmen abgefragt und verwendet werden (Einsichtsfähigkeit). Dies hängt direkt mit dem Grad der Entwicklung und damit auch mit dem Alter zusammen. Daher geht das Einwilligungsrecht graduell von den Eltern auf die Kinder über.

Checkliste

× Vorab: Für welche Altersgruppe ist das Angebot gedacht?

Es ist vorab zu klären, welche Altersgruppe mit dem Angebot angesprochen werden soll.

× Keine Besonderheiten für Jugendliche, die das 16. Lebensjahr vollendet haben

Jugendliche ab 16 Jahren können in dieser Hinsicht wie Erwachsene behandelt werden. Für sie gelten keine Besonderheiten. Sie können ohne Mitwirkung der Eltern in eine Datenverarbeitung

einwilligen; ebenso können sie ihre Einwilligung auch jederzeit selbst widerrufen. Im Übrigen gelten sämtliche datenschutzrechtlichen Vorgaben und Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung usw. – vgl. ***Datenschutz „Basics"***).

× Einzelabwägung bei Jugendlichen von 13 bis 16 Jahren

Bei 13- bis 16-Jährigen hängt die Möglichkeit einer eigenen wirksamen Einwilligung vom Grad der Reife und dem Zweck der Einwilligung und der damit einhergehenden Tragweite der Entscheidung in die Datenpreisgabe ab. Maßgeblich ist die individuelle Einsichtsfähigkeit. Insofern kommt es in dieser Altersgruppe immer auf den Einzelfall an.

Es ist dabei zu berücksichtigen, dass der durchschnittliche Jugendliche in dieser Altersgruppe mit Computer, Internet und Social Media aufgewachsen ist und regelmäßig schon Erfahrungen im Umgang mit dem Internet gesammelt hat. Ab Vollendung des 13. Lebensjahrs kann i.d.R. von einer Einsichtsfähigkeit ausgegangen werden, wenn transparent und altersgerecht über die Art und den Zweck der Datenverarbeitung aufgeklärt wird.

Entscheidend ist auch der Zweck der Datenabfrage. Danach sollte es für Kinder und Jugendliche beispielsweise möglich sein, einen Newsletter der Lieblingswebseite zu abonnieren oder sich auf einer Lernplattform zu registrieren.

Es wird empfohlen, z.B. einen spielerischen Zugang zu wählen und damit die Einsichtsfähigkeit „abzuprüfen". Die Teilnahme bei einem Datenschutzspiel und den damit verbundenen Lösungen von Aufgaben kann die Voraussetzung für die Nutzung eines Angebotes sein.

Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung, Datensicherheit usw. – vgl. ***Datenschutz „Basics"***).

× Achtung bei Kinder unter 13 Jahren: Einwilligung der Eltern erforderlich

Bei Kindern unter 13 Jahren muss eine Einwilligung der Eltern eingeholt werden. Dies gestaltet sich in der Praxis nicht immer leicht. Am sichersten ist der schriftlich-postalische Weg, auch wenn dieser dem Medium Internet nicht gerecht wird und sehr aufwändig ist. Möglich sind auch digitale Einwilligungsformen, beispielsweise die Zusendung eines digitalen Fotos der unterschriebenen Einwilligungserklärung. Häufig werden für die Einwilligung Klick-Boxen eingesetzt. Hier müssen Kinder die E-Mail-Adresse der Eltern angeben und diese müssen dann der Datenverwendung zustimmen (sog. „Eltern-Okay"). Jedoch können Kinder natürlich auch ihre E-Mail-Adresse hier angeben und demnach selbst zustimmen. Dieses Verfahren ist also nicht vollständig sicher, weil es durch den Minderjährigen umgangen werden kann. Wenn die Einwilligung der Eltern erforderlich ist, muss diese auch nachgewiesen werden.

Im Hinblick auf die praktischen Schwierigkeiten bei der Einwilligung der Eltern ist immer auch zu prüfen, ob Mitmachaktionen u.ä. auch gänzlich ohne personenbezogene Daten realisiert werden können.

Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung, Datensicherheit usw. – vgl. ***Datenschutz „Basics"***).

× Absolutes Muss: Kinderfreundliche Datenschutzerklärung

Wenn Minderjährige einsichtsfähig sind und damit selbst einwilligen können, ist es von entscheidender Bedeutung, dass ihnen auch die erforderlichen Informationen gegeben werden. Die Datenschutzerklärung muss leicht auffindbar und in einfacher Sprache verständlich gefasst sein. Die einzelnen Einwilligungen in die Datenverarbeitung müssen ebenfalls so gestaltet sein, dass der Minderjährige erkennt, worin er tatsächlich einwilligt.

Gleiches gilt für Angebote an Kinder bis 13 Jahre: Bei der Erhebung von Daten bei Kinderangeboten spielt die Transparenz eine große Rolle. Je klarer dem Kind und auch den Erziehungsberechtigten die Notwendigkeit der Daten für das Produkt verdeutlicht wird, umso größer wird die Akzeptanz für die Erhebung. Ebenso sollte in den Datenschutzhinweisen erklärt werden, wie lange die Daten für den Zweck vorgehalten werden, dass sie abschließend gelöscht werden, usw.. Es gelten insoweit die Hinweise zur ***Datenschutzerklärung***.

× Keine Einwilligung bei Präventions- und Beratungsdiensten direkt für Kinder und Jugendliche

Im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind oder Jugendlichen angeboten werden, ist die Einwilligung der Eltern generell nicht erforderlich (Besonderheit des neuen EU-Rechts). Das Konzept des Angebotes sollte daher auf seine medienpädagogische Relevanz geprüft werden. Dient es auch der Prävention oder Beratung der Kinder/Jugendlichen?

× Abstimmung mit dem Datenschutzbeauftragten

Wegen der Besonderheiten des Minderjährigen-Datenschutzes wird empfohlen, sich bei allen Konzepten, Projekten und Angeboten immer mit dem jeweiligen Datenschutzbeauftragten zu beraten und abzustimmen.

× Förderung der Medienkompetenz und Einsichtsfähigkeiten der Kinder und Jugendlichen

Bei allen Angeboten für Minderjährige sollten die Rundfunkanstalten einen Beitrag zur Bildung von Medienkompetenz bei Kindern und Jugendlichen leisten. Gerade bei dieser Altersgruppe gibt es vielfache Möglichkeiten, die Einsichtsfähigkeit durch Spiele u.ä. zu „trainieren".

PERSONALISIERUNG

Über die Personalisierung einer Webseite kann dem Nutzer ein jeweils auf seine Vorlieben und Interessen individuell zugeschnittenes Angebot zur Verfügung gestellt werden.

Derzeit etablieren sich am Markt Funktionalitäten, die dem Nutzer zielgerichtete, auf seine Präferenzen abgestimmte Angebote machen können (Merklisten, Playlists, Empfehlungen, Push-Nachrichten, Social-Media-Einbindung etc.).

Hierfür werden alle dafür nützlichen Daten ausgewertet und die jeweilige Webseite wird entsprechend angepasst und angezeigt, z.B. mit Hilfe von Cookies und persönlichen Daten, die bei einer Registrierung aufgenommen wurden. Diese Personalisierungsfunktionen können teilweise nur angeboten werden, wenn der Nutzer sich bei einem Dienst anmeldet bzw. seine Daten in einem gewissen Umfang zur Verfügung stellt.

Was sagt der Datenschutz?

Für eine Personalisierung müssen in der Regel Informationen über das Verhalten des Nutzers gesammelt werden, um ihm Vorschläge zum Angebot zu unterbreiten oder ihm die Möglichkeit zu bieten, sich sein eigenes Angebot zusammenzustellen. Diese Informationen können Personenbezug aufweisen oder nicht. Für die Anwendung des Datenschutzrechts kommt es also darauf an, welche und wie viele Daten jeweils tatsächlich genutzt werden.

Generell sollte bei der Personalisierung mit Fingerspitzengefühl und Sorgfalt vorgegangen werden.

Checkliste

× Personalisierung durch persönliches Nutzerkonto

Personalisierung kann dadurch erreicht werden, dass der Nutzer sich freiwillig für ein eigenes Konto mit persönlichen Daten, Vorlieben und Interessen registriert. Der Nutzer muss sich hier

über ein eigenes Login anmelden und kann sein Konto einsehen und selbst verwalten. Auf diese Weise bekommt er nur für ihn zugeschnittene Inhalte angeboten, die er auf sämtlichen Endgeräten nutzen kann. In diesem Fall gelten die bekannten Datenschutzprinzipien (siehe *Datenschutz „Basics"*):

» Einwilligung

Der Nutzer muss explizit in die Erhebung und Verwendung seiner Daten einwilligen. Dafür braucht es eine transparente Aufklärung sowie eine Dokumentation der Einwilligungserklärung. Es ist darauf zu achten, dass diese Einwilligungserklärung stets abgerufen und auch widerrufen werden kann.

» Datensparsamkeit, Zweckbindung, Löschung, Datensicherheit

Für personalisierte Funktionalitäten sollen nur die Daten der Nutzer erhoben werden, wie sie für die spezifischen Angebote notwendig, redaktionell intendiert und vom Nutzer gewollt sind. Das Sammeln von Daten auf Vorrat ist unzulässig. Pflichtfelder und Felder für freiwillige Angaben des Nutzers müssen daher klar gekennzeichnet sein.

Die Daten dürfen nur zu dem vorher klar festgelegten Zweck verwendet werden und dürfen nicht zu anderen Zwecken genutzt oder an Dritte weitergegeben werden. Sie müssen nach Abmeldung oder bei Widerruf der Einwilligung wieder gelöscht werden.

Das Angebot sollte immer die Option bieten, sich von Nutzungsmessungen und Personalisierungsfunktionen abzumelden.

Sehr wichtig ist die sichere Datenhaltung: Vertraulichkeit, Integrität und Verfügbarkeit der Accounts und Nutzerdaten müssen durch entsprechende Vorkehrungen sichergestellt sein.

× Personalisierung über Pseudonymisierung/Anonymisierung

Werden personenbezogene/-beziehbare Daten eines Nutzers pseudonymisiert oder anonymisiert, kann die Identität des Nutzers nicht mehr nachvollzogen werden. Es werden lediglich Unterscheidungsmerkmale gespeichert, so dass auf diese Weise ein individualisiertes Angebot ermöglicht wird. Der einzelne Nutzer ist nicht mehr identifizierbar.

In diesem Fall ist auf folgendes zu achten:

» Wirksame Pseudonymisierung/Anonymisierung

Es ist z.B. möglich, über eine Geräte-ID oder die IP-Adresse Daten über das Verhalten zu sammeln, um individuelle Empfehlungen auszusprechen. Aber Vorsicht: IP-Adresse und Gerätekennung gelten als personenbezogene Daten. Daher sollten Optionen genutzt werden, die IP-Adresse zu pseudonymisieren oder für die Gerätekennung eine zufallsgenerierte eindeutige Nummer (Token) zu erzeugen, der im Rahmen der Nutzung eindeutig ist, aber außerhalb der App keinen Bezug zum Gerät mehr aufweist.

» Möglichkeit des Widerspruchs bei Bildung pseudonymer Nutzerprofile

Sofern zum Zweck der Personalisierung pseudonyme Nutzerprofile gebildet werden, muss der Nutzer die Möglichkeit bekommen, der Bildung von Nutzerprofilen zu widersprechen (siehe hierzu

die Hinweise zur ***Web-Analyse***).

× Immer: Umfassende Informationen in der Datenschutzerklärung

Für alle Formen der Personalisierung gilt: Die Rundfunkanstalt muss in der Datenschutzerklärung ihres Angebots umfassend und verständlich über Art und Verwendungszweck der Daten aufklären. Auch die Verwaltung der Nutzerdaten sollte erklärt werden.

× Minderjährigen-Datenschutz

Sofern sichergestellt ist, dass keine personenbezogenen Daten erhoben werden und der Minderjährige nicht identifiziert werden kann, ist grundsätzlich für Minderjährige ein individuell zugeschnittenes Angebot denkbar. Es sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

SOCIAL LOGIN

Social Login wird auch als Social Sign-In bezeichnet. Viele soziale Netzwerke wie Facebook, Twitter und Google+ bieten Betreibern von Webseiten oder Apps für einen Registrierungs-prozess einen geschützten Bereich, damit sich die Nutzer (alternativ) mit ihrem Facebook-, Google- oder Twitter-Account anmelden können. Den Nutzern erspart dies zusätzliche Passwörter und Logins.

Was sagt der Datenschutz?

Klickt der Nutzer auf den Social-Login-Button und meldet sich z.B. über seinen Facebook-Account an, erfolgt die Verknüpfung von Facebook und der Webseite, worüber Facebook stets das öffentliche Profil (insb. Name, Profil, Geschlecht) und die Freundesliste übermittelt, da diese Informationen als „öffentlich" eingestuft sind. Dazu können noch weitere Daten übermittelt werden, die vom Nutzer im Rahmen seiner Privatsphäre-Einstellungen nicht explizit eingeschränkt wurden. Im Gegenzug erhält Facebook Informationen zur Nutzung der Seite durch den Nutzer. Diese Daten können dem Facebook-Benutzerprofil beigefügt und von Facebook weiterverarbeitet werden (z.B. Auswertung der Daten zu Werbezwecken).

Die Funktionalität des Social Logins wurde durch die Betreiber der sozialen Netzwerke entwickelt; diese sind daher für die datenschutzkonforme Datenübermittlung an den jeweiligen Webseitenbetreiber verantwortlich.

Aber: Auch die Rundfunkanstalt, die Social Login in ihren Apps und Webseiten anbietet, bleibt datenschutzrechtlich verantwortlich für den Bezug und die Weitergabe von Daten der Nutzer auf/von ihren Angeboten an Facebook u.a.

Beim Einsatz von Social Logins hängt die Zulässigkeit dieser Datenverarbeitungen regelmäßig von einer wirksamen Einwilligungserklärung des Nutzers ab. Diese muss vor der Inanspruchnahme des Social Login eingeholt werden.

Angesichts der intransparenten Datennutzung der sozialen Netzwerke, namentlich Facebook, besteht das Risiko, dass das Social Login insgesamt rechtlich unzulässig ist. Auch wenn Facebook seine Nutzer über den Datentransfer aufklärt, genügt dies möglicherweise nicht den gesetzlichen Vorgaben in Deutschland an eine aufgeklärte und transparente Einwilligung.

Checkliste

× Information und Einwilligung unmittelbar beim Social Login

Vor Abschluss des Registrierungsvorgangs via Social Login ist der Nutzer über eine eigene zustimmungspflichtige Datenschutzerklärung zu informieren, welche Daten konkret in der Folge von dem sozialen Netzwerk und an dieses und zu welchen Zwecken übermittelt werden. Es empfiehlt sich eine Einbindung der Hinweise im Log-in-Dialog bzw. in unmittelbarer Nähe des Social-Login-Button. Möglich ist dabei eine Verlinkung, so dass der Nutzer per Klick zur unternehmenseigenen Datenschutzerklärung gelangt, in der er über den Log-in-Prozess aufgeklärt wird.

× Hinweis zum Social Login in eigener Datenschutzerklärung

Neben der Einholung einer Einwilligung muss die Datenschutzerklärung über das Social-Login-Verfahren und die ablaufenden Datenprozesse aufklären.

Hier genügt nicht der Hinweis darauf, dass die Social-Login-Funktion den Bestimmungen und der Verantwortung des sozialen Netzwerkes unterliegt. Insbesondere sollte erläutert werden, welche Daten vom sozialen Netzwerk bezogen und zu welchen Zwecken diese Daten verwendet werden.

Sofern die Rundfunkanstalt Daten an das soziale Netzwerk sendet, sind diese aufzulisten und darüber zu informieren, zu welchen Zwecken das Netzwerk diese Daten nutzt. Schließlich sollte erklärt werden, wie die Verknüpfung zwischen der Webseite der Rundfunkanstalt und dem sozialen Netzwerk wieder gelöst werden kann.

× Alternative Registrierungsmöglichkeit

Dem Nutzer sollte es immer freigestellt werden, zwischen dem Social Login und einer separaten Registrierungsmöglichkeit frei zu wählen.

STANDORTDATEN

Standortdaten (Geodaten) sind Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts angeben, mit dem ein Telekommunikationsdienst genutzt wird. Insbesondere Smartphones und Tablets können durch verschiedene Techniken - GPS, WLAN, das Mobilfunknetz oder via IP-Adresse - die Position des Nutzers ermitteln.

Das machen sich viele Apps zu eigen und bieten Lokalisierungsdienste an. Wenn Dienste Geodaten berücksichtigen, ist das häufig hilfreich, indem sie passgenaue Informationen liefern. Mit Hilfe dieser Daten können den Nutzern ausgewählte Meldungen und Informationen übermittelt werden, die sich auf ihre nähere Umgebung beziehen, z.B. Angaben zum ortsbezogenen Geschehen, Wetter, Verkehr oder zu kulturellen Ereignissen in der Region. Auf der anderen Seite geben Standortdaten Aufschluss über die „Bewegungen", Gewohnheiten und Interessen der Nutzer.

Was sagt der Datenschutz?

Bei der Ermittlung von ortsbezogenen Daten wird streng genommen nie der jeweilige Nutzer selbst, sondern immer das zugehörige Gerät mit mehr oder weniger großer Genauigkeit geographisch bestimmt. Gleichwohl besteht das Risiko, dass die Standortdaten bestimmbaren Personen zugeordnet werden können, wenn sie z.B. mit der jeweiligen IP-Adresse der Nutzer übermittelt bzw. gespeichert werden.

Durch die Sammlung und Verknüpfung von unterschiedlichen Standortdaten ist es möglich, Bewegungsprofile zu erstellen. Dadurch kann festgestellt werden, wann und wie lange eine Person an einem bestimmten Standort war. Auch Ortungsdaten in anonymisierter Form lassen sich z.B. mit weiteren Datenbeständen kombinieren und so wieder einzelnen Nutzern zuordnen. Einige Dienste sammeln Standortdaten über das notwendige Maß hinaus im Hintergrund und ohne Wissen und Wollen des Nutzers. Regelmäßig werden die Daten zur weiteren kommerziellen Nutzung auch an Dritte weitergegeben.

Die Erhebung und Verwendung von solchen personenbeziehbaren Daten ist nur dann zulässig, soweit die Daten erforderlich sind, um die Inanspruchnahme des Dienstes zu ermöglichen oder wenn die Nutzer dem im Vorwege zugestimmt haben.

Checkliste

Wenn eine Rundfunkanstalt Standortdaten erheben will (z.B. für einen Lokalisierungsdienst in einer App), ist auf Folgendes zu achten:

× Information und Einwilligung vor bzw. bei Beginn der Nutzung / Deaktivierung

Die Erhebung und Verwendung von Standortdaten durch die Rundfunkanstalt muss stets vorab von den Nutzern nach einer entsprechenden Information freigegeben werden.

Darum ist eine etwaige Lokalisierungsfunktion eines Angebots - z.B. eine App einer Rundfunkanstalt - in den Voreinstellungen standardmäßig zu deaktivieren. Daneben muss es den Nutzern nach Aktivierung möglich sein, die gewählte Funktion jederzeit wieder abzuschalten. Aktivierung und Deaktivierung sollten möglichst durch nur einen Klick erfolgen können.

× Informationen zur Erhebung der Standortdaten und zur Aktivierung / Deaktivierung

Die Nutzer sind vorab genau über Art, Umfang und Zweck der Erhebung und Verwendung der Standortdaten zu informieren. Das kann beispielsweise innerhalb der Datenschutzerklärung erfolgen, der vor Beginn der Nutzung des Dienstes zuzustimmen ist. Außerdem muss die Möglichkeit der jederzeitigen Aktivierung bzw. Deaktivierung dieser Datenerhebung aufgezeigt und erklärt werden.

× Datensparsamkeit: Erhebung und Nutzung nur der notwendigen Daten

Mit Beginn der Nutzung der Dienste muss sichergestellt sein, dass die Daten nach dem Grundsatz der Datensparsamkeit lediglich erhoben werden, soweit sie zur Nutzung des Dienstes notwendig sind.

Standortdaten können auch permanent und in regelmäßigem Turnus - z.B. alle dreißig Minuten - erhoben werden, um Nutzern einen bestimmten Dienst bieten zu können (z.B. Stau- und Blitzermeldungen als Push-Nachricht). Der Nutzer ist hierüber zu informieren bzw. hat hierzu seine Einwilligung zu geben.

Eine dauerhafte Speicherung von Standortdaten auf dem Endgerät darf nur dann stattfinden, wenn dies für die Funktionalität des Dienstes notwendig ist. Gleiches gilt in Bezug auf die Informationen, die an die Anbieter der Dienste gesendet werden. Andernfalls würde auch hier die Gefahr der Erstellung von Bewegungsprofilen bestehen.

× Sofern möglich: „Verwaschung" des Standorts

Häufig ist es nicht notwendig, dass der Standort des Nutzers metergenau erhoben und verwendet wird. Darum empfiehlt sich eine gezielte „Verwaschung" des Standortes. Dies kann z.B. durch eine Nullung von Dezimalstellen in den GPS-Koordinaten vor Versand der Daten an den jeweiligen Dienste-Anbieter erreicht werden.

× Wichtige Hinweise für die Löschung der Dienste

Wenn die Daten lokal gespeichert werden, ist dafür Sorge zu tragen, dass nach der Löschung des (Lokalisierungs-)Dienstes auch die lokal gespeicherten personenbezogenen Daten des Nutzers gelöscht werden.

Sollte es sich dabei um Daten handeln, die z.B. auch anderen Apps auf dem Endgerät zur Nutzung zur Verfügung gestellt werden, sollte der Nutzer bei der Deinstallation gezielt gefragt werden, ob er diese persönlichen Daten löschen oder auf dem Gerät belassen möchte.

VOTINGS

Votings (Nutzerabstimmungen) sind für viele Redaktionen ein attraktives Element der Programmgestaltung. Durch den direkten Rückkanal sollen die Nutzer am Programm und der Gestaltung des Onlineangebots teilhaben.

Bei der konkreten Ausgestaltung gibt es zahlreiche Varianten („Welche Filme sollen in der Märchenreihe gezeigt werden?", „Schönste Brücke von XY?"). Dies gilt auch für die technische Umsetzung. Es gibt Votings im eigenen Angebot der Rundfunkanstalt, die in der Regel auch On-Air beworben werden, einschließlich Mitmachmöglichkeiten im eigenen Angebot und/oder Drittplattformen. Es gibt aber auch Votings, die ausschließlich auf Drittplattformen durchgeführt werden (z.B. „Liken und teilnehmen").

Was sagt der Datenschutz?

Welche Nutzerdaten wie lange bei einem Voting verarbeitet werden, hängt von der konkreten Ausgestaltung des Votings ab. Daher ist es wichtig, vorab Ablauf und Bedingungen für das Voting festzulegen und die Nutzer hierüber ausreichend zu informieren. Es sind so wenig Nutzerdaten wie möglich zu erheben.

Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es für die Durchführung des Votings erforderlich ist. Sie dürfen auch nicht anderweitig verwendet werden. Danach ist eine Löschung erforderlich.

Checkliste für Votings im anstaltseigenen Angebot

× Zweckbindung und Datensparsamkeit

Es sind so wenig Nutzerdaten wie möglich zu erheben: Zulässig sind nur die Daten, die für die Durchführung des Votings unbedingt notwendig sind (kein „nice to have"). Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es für die Durchführung des Votings erforderlich ist. Sie dürfen für keine anderen Zwecke verwendet werden.

× Informationen in der Datenschutzerklärung

Vorab sind Ablauf und Bedingungen für das Voting festzulegen und hierüber in den Datenschutzhinweisen zu informieren.

× Absicherung gegen Manipulation

Bei internetbasierten Abstimmungsformen kann - unter Berücksichtigung der Nutzerfreundlichkeit - eine technische Absicherung gegen Manipulation von außen eingesetzt werden (z.B. durch Sperrung der IP-Adresse für ein bestimmtes Zeitfenster, Captcha, Identifizierung per Mail, Cookies). In diesem Fall sind nur solche Daten der Nutzer mitzuloggen, die für die korrekte Durchführung des Votings erforderlich sind. Zudem ist ein konkreter Hinweis in der Datenschutzerklärung erforderlich.

× An die Löschung denken

Es sind Löschfristen festzulegen und darauf zu achten, dass die Daten gelöscht werden, sobald das Voting beendet und eine angemessene „Reklamationszeit" einkalkuliert wurde. Die Daten sind notfalls manuell zu löschen.

× Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur in der Rundfunkanstalt verarbeitet und gespeichert werden. Sofern ein Dienstleister mit der Durchführung und/oder dem Hosting eines Votings beauftragt ist, sind die Hinweise zur ***Auftragsvergabe an Dritte*** zu beachten.

× Verknüpfung mit Gewinnspiel

Eine Teilnahme am Voting kann mit einem Gewinnspiel kombiniert werden (z.B. „Unter den ‚Votern' werden Tickets verlost."). In diesem Fall sind zusätzlich die Hinweise zu ***Gewinnspielen*** zu beachten.

× Verschlüsselung

Die Kommunikation mit Nutzern über das Internet ist so sicher wie möglich zu gestalten, sobald persönliche Daten übertragen werden – dies gilt auch bei Votings. Insofern sollte stets eine verschlüsselte Übertragung ermöglicht werden, sofern dies technisch realisierbar und vom Aufwand her verhältnismäßig ist.

× Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum ***Minderjährigen-Datenschutz*** zu beachten.

Checkliste für Votings ausschließlich auf Drittplattformen

× Verantwortlichkeit des Plattformanbieters

Es gelten grundsätzlich die Datenschutzbestimmungen des jeweiligen Plattformanbieters (siehe hierzu auch die Hinweise unter ***Drittplattformen***).

× Achtung bei Nutzerverarbeitung auch durch die Rundfunkanstalt

Sobald die Nutzerdaten anlässlich des Votings auch in der Rundfunkanstalt verarbeitet werden, gelten die o.g. Vorgaben.

× Beachtung der sonstigen Vorgaben der Drittplattform

Es sind die sonstigen AGB/Richtlinien zur Veranstaltung von Votings durch Unternehmen zu beachten (vgl. z.B. die Regelung zu „Promotionen" in den Nutzungsbedingungen von Facebook ***www.facebook.com/page_guidelines.php***).

WEB-ANALYSE

Web-Analyse (genannt auch Traffic-Analyse, Webtracking oder Webcontrolling) ist die Sammlung von Daten und deren Auswertung bezüglich des Verhaltens von Besuchern auf Webseiten. Ein Webanalyse-Tool untersucht, woher die Besucher kommen, welche Bereiche auf einer Seite aufgesucht werden und wie oft und wie lange welche Unterseiten und Kategorien angesehen werden.

Es gibt verschiedene Analyse-Verfahren (z.B. Piwik, INFOnline, Comscore). Gewöhnlich werden entweder die Logdateien der Webserver ausgewertet oder bestimmte Zählpixel oder Tags in Webseiten zur Datengewinnung genutzt. Cookies sind dabei unabdingbar, um einen Seitenaufruf einer Sitzung und eine Sitzung einem Besucher zuordnen zu können.

Was sagt der Datenschutz?

Bei Web-Analyseverfahren können personenbezogene Daten anfallen, so z.B. auch die

IP-Adresse des Nutzers. Hierfür ist grundsätzlich die Einwilligung des Nutzers erforderlich.

Zu Zwecken der Marktforschung und zur bedarfsgerechten Gestaltung von Webseiten dürfen jedoch auch ohne Einwilligung Nutzungsprofile erstellt werden, sofern diese pseudonymisiert sind und der Nutzer dem nicht widerspricht.

Checkliste

× Personenbezogene Nutzungsprofile nur mit Einwilligung

Die Erstellung personenbezogener Nutzungsprofile ist grundsätzlich nur mit bewusster, eindeutiger Einwilligung des Nutzers zulässig.

× Vorsicht bei IP-Adressen

Die vollständige IP-Adresse ist ein personenbezogenes Datum. Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist daher nur mit Einwilligung des Nutzers zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

× Pseudonyme Nutzerprofile ohne Einwilligung zulässig

Die Erstellung von Nutzungsprofilen zur Werbung und zur Marktforschung ist gesetzlich erlaubt, sofern drei Voraussetzungen beachtet werden:

» Pseudonyme:

Es müssen Pseudonyme verwendet werden. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym - zumeist eine mehrstellige Buchstaben- oder Zahlenkombination (Code) - ersetzt, um die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren.

» Widerspruchsrecht:

Dem Nutzer ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Zudem muss der Nutzer in der Datenschutzerklärung auf sein Widerspruchsrecht gegen die Erstellung von Nutzungsprofilen hingewiesen werden.

» Strikte Datentrennung:

Das Nutzungsprofil darf nicht mit dem Träger des Pseudonyms zusammengeführt werden. Diese Daten müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

× Anonyme Nutzungsprofile unterliegen nicht dem Datenschutz

Anonyme Auswertungen unterliegen – mangels Personenbezug – keiner datenschutzrechtlichen Beschränkung. Bei der Erstellung anonymer Nutzungsprofile muss allerdings die Anonymität bereits bei der Erhebung der Information, beispielsweise des Klick-Verhaltens, gegeben sein.

× Pflicht zur Information in der Datenschutzerklärung

Die Rundfunkanstalt muss im Rahmen der Datenschutzerklärung auf ihrer Internetseite in deutlicher Form auf die Erstellung von Nutzungsprofilen und den Zweck und Umfang der Datenspeicherung hinweisen.

Zudem muss der Nutzer hier auf das Widerspruchsrecht hingewiesen und eine Möglichkeit geschaffen werden, dieses Widerspruchsrecht unmittelbar auszuüben. Es bietet sich an, einen Link vorzusehen, bei dem eine direkte Opt-out-Funktion hinterlegt ist.

× Achtung beim Einsatz von Cookies

Regelmäßig werden bei Tracking-Technologien auch (permanente) Cookies eingesetzt. Hierauf muss in der Datenschutzerklärung hingewiesen werden. Zudem sollte darüber informiert werden, wie Cookies bei den gängigen Browsern deaktiviert werden können. Es gelten im Einzelnen die Hinweise zu ***Cookies***.

× Achtung: Auftragsdatenverarbeitung!

Die Web-Analyse wird meistens durch Drittanbieter vorgenommen. Daher ist es unbedingt notwendig, die Vorgaben zur Auftragsdatenverarbeitung einzuhalten, sofern die vollständigen IP-Adressen und sonstige Nutzerdaten bei dem Dritten erhoben und verarbeitet werden. Es sind die Hinweise zur ***Auftragsvergabe an Dritte*** zu beachten.

» Herausgeber: Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio

» Redaktion: Barbara Nickel, Bayerischer Rundfunk

» Design: Henrik Ullmann, Bayerischer Rundfunk – Abt. Multimedia Design

» Stand: September 2016

Anlage 3

rbb	Rundfunk Berlin-Brandenburg
AD	Active Directory
aF	alte Fassung
AGF	Arbeitsgemeinschaft Fernsehforschung
AK DSB	Arbeitskreis der Datenschutzbeauftragten
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BerlGSG	Berliner Datenschutzgesetz (nF)
BerlHG	Berliner Hochschulgesetz
BlnDSG	Berliner Datenschutzgesetz (aF)
BlnMDÜV	Verordnung zur Übermittlung von Meldedaten in Berlin
BMG	Bundesmeldegesetz
BVerfG	Bundesverfassungsgericht
BVG	Berliner Verkehrsbetriebe
BYOD	Bring your own device
DFL	Deutsche Fußballliga GmbH
DRL	Deutschlandradio
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkonferenz
DVO-MeldeG	Verordnung zur Durchführung des Meldegesetzes
EAID	Europäische Akademie für Informationsfreiheit und Datenschutz
EUDAGO	Umsetzung der Anforderungen aus der EU-Datenschutzgrundverordnung
EU-DSGVO	Europäische Datenschutzgrundverordnung
Europäischer Gerichtshof	EuGH
HGB	Handelsgesetzbuch
hr	Hessischer Rundfunk
HSB	ARD-Hauptstadtstudio
ISB	Informationssicherheitsbeauftragter
ISK	Informationssicherheitskreis
ISMS	Informations-Sicherheits-Management-System
IT	Informationstechnik
IVZ	Informationsverarbeitungszentrum
KEF	Kommission zur Ermittlung des Finanzbedarfs
LAG	Landesarbeitsgericht
LG	Landgericht
LGG	Landesgleichstellungsgesetz
MDR	Mitteldeutscher Rundfunk
MeldDÜV	Brandenburgische Meldedatenübermittlungsverordnung
MiMa	Mittagsmagazin
NDR	Norddeutscher Rundfunk
nF	neue Fassung
NRW	Nordrhein Westfalen
OLG	Oberlandesgericht
OTT-Dienste	Over-the-Top-Dienste
OuI	Abteilung Organisation und Informationstechnik
OVG	Oberverwaltungsgericht
PresseG Bln	Pressegesetz Berlin
RÄndStV	Rundfunkänderungsstaatsvertrag
RB	Radio Bremen
RBStV	Rundfunkbeitragsstaatsvertrag
rbt	Rundfunk-Betriebstechnik GmbH
RBT	ARGE Rundfunk-Betriebstechnik
RL	Richtlinie
RStV	Rundfunkstaatsvertrag
SaaS	Software as a Service
SR	Saarländischer Rundfunk
SWR	Südwestrundfunk
TKG	Telemedienkommunikationsgesetz
TMG	Telemediengesetz
UC	Unified Communication
VBB	Verkehrsverbund Berlin-Brandenburg
VPMS	Video Produktions Management System
VVT	Verzeichnis von Verarbeitungstätigkeiten
VwGO	Verwaltungsgerichtsordnung
WDR	Westdeutscher Rundfunk
ZBS	ARD ZDF Deutschlandradio Beitragsservice
ZDF	Zweites Deutsches Fernsehen