


**SWR** >>



**DATEN  
SCHUTZ  
IM FOKUS**

**12. TÄTIGKEITSBERICHT  
DES DATENSCHUTZBEAUFTRAGTEN**

1. Januar – 31. Dezember 2019 • Prof. Dr. Armin Herb



**12.Tätigkeitsbericht  
des Rundfunkbeauftragten  
für den Datenschutz  
des Südwestrundfunks**

**Prof. Dr. Armin Herb**

**Berichtszeitraum: 1.1.2019 bis 31.12.2019**

Veröffentlicht und erstattet gemäß Art. 59 der EU-DSGVO 2016/679 i.V.m. § 39 Abs. 1 SWR-StV i.V.m. § 27 Abs. 10 LDSG BW vom 12.6.2018 (GBl. BW 2018 S. 173 ff.) dem Rundfunkrat, dem Verwaltungsrat, dem Intendanten des SWR sowie den Landtagen und Landesregierungen Baden-Württemberg und Rheinland-Pfalz.

## INHALTSVERZEICHNIS

<b>ZUSAMMENFASSENDE WÜRDIGUNG .....</b>	<b>5</b>
<b>1 ENTWICKLUNG DES DATENSCHUTZRECHTS IM JAHR 2019 .....</b>	<b>7</b>
1.1 EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG.....	7
1.2 WEITERE EUROPÄISCHE VERORDNUNGEN UND RICHTLINIEN ZUM DATENSCHUTZ.....	8
1.2.1 <i>E-Privacy-VO als Nachfolge der RiLi 2002/58 zur elektronischen Kommunikation .....</i>	<i>8</i>
1.2.2 <i>EU-Verordnung zur Cybersicherheit vom 17.4.2019 .....</i>	<i>8</i>
1.2.3 <i>EU-Verordnung vom 20. Juni 2019 zu Online-Vermittlungsdiensten .....</i>	<i>8</i>
1.2.4 <i>EU-Richtlinie zum Schutz von Personen, die Verstöße melden vom 23.10.2019 .....</i>	<i>9</i>
1.3 GESETZGEBUNG IM BEREICH DES BUNDES.....	10
1.3.1 <i>Bundesdatenschutzgesetz II vom 20.11.2019 .....</i>	<i>10</i>
1.3.2 <i>Gesetz zum Schutz von Geschäftsgeheimnissen vom 18.4.2019.....</i>	<i>11</i>
1.3.3 <i>Gesetz des Bundes zur Kontrolle von Diesel-Fahrverboten vom 8.4.2019 .....</i>	<i>11</i>
1.3.4 <i>Gesetzentwurf zu Abmahnverfahren .....</i>	<i>11</i>
1.4 GESETZGEBUNG IM BEREICH DER ZUSTÄNDIGKEIT DER LÄNDER .....	12
1.4.1 <i>Rundfunkstaatsverträge .....</i>	<i>12</i>
1.4.2 <i>Rundfunkfinanzierungs-Staatsvertrag .....</i>	<i>13</i>
1.5 DATENSCHUTZRICHTLINIE DES EUROPARATES (KONVENTION 108).....	13
<b>2 DATENSCHUTZ IM PROGRAMM- UND PRODUKTIONSBEREICH DES SWR .....</b>	<b>14</b>
2.1 TIKTOK – DER 15-SEKUNDEN-WAHN BEI JUGENDLICHEN.....	14
2.2 WHATSAPP .....	15
2.3 TWITTER ABGESCHALTET.....	16
2.4 ÄRGER UM SCRIBBLELIVE.....	16
2.5 SWR3 PUSHED .....	17
2.6 ONSITE-BEFragung BEI SWR 3 .....	18
2.7 DIE WEBCAM AM BODENSEE .....	18
2.8 VIEL LÄRM UM DEN DATENSCHUTZ.....	19
2.9 WARNUNG VOR TRICKBETRUG.....	19
2.10 MEDIALOOPSTER FÜR FUNK .....	20
2.11 EVA UND DER DATENSCHUTZ.....	21
2.12 „APPLAUS FÜR @SWRPRESSE UND FUNK“ .....	22
2.13 UMFragEN – WAS GILT ES ZU BEACHTEN?.....	23

<b>3</b>	<b>DATENSCHUTZ IM VERWALTUNGSBEREICH DES SWR .....</b>	<b>25</b>
3.1	DER SPLITTER IM AUGE DER ZUSCHAUER UND DER BALKEN IM EIGENEN AUGE - DIE OFFENEN WUNDE VERTRAULICHKEITSERKLÄRUNG.....	25
3.2	VERTRAULICHE LEIHARBEIT? .....	25
3.3	TOPFIT IM DATENSCHUTZ? .....	26
3.4	GYMPASS .....	27
3.5	EABRECHNUNG ENDLICH SICHER.....	28
3.6	DES PUDELS KERN.....	28
3.7	DATENSCHUTZ BEI DER SWR MEDIA SERVICES GMBH .....	29
3.7.1	<i>Die Mutter aller Türme.....</i>	29
3.7.2	<i>Datensicherheit.....</i>	29
<b>4</b>	<b>DATENSCHUTZ BEIM ARD ZDF DEUTSCHLANDRADIO BEITRAGSSERVICE.....</b>	<b>30</b>
4.1	GRUNDLAGEN ZUM RUNDFUNKBEITRAG .....	30
4.2	DATENBESTAND BEIM ZENTRALEN BEITRAGSSERVICE UND BEIM SWR .....	31
4.3	MELDEDATENABGLEICH.....	31
<b>5</b>	<b>DATENSICHERHEIT IM SWR.....</b>	<b>33</b>
5.1	PHISHINGVERSUCHE DURCH GEFÄLSCHTE E-MAILS .....	33
5.2	ANGRIFF AUF EINEN SWR-SERVER .....	33
5.3	SICHERHEITSPROBLEME BEI IPHONES UND IPADS .....	34
5.4	ANGRIFFE AUF EINEN DIENSTLEISTER.....	34
<b>6.</b>	<b>AUSKUNFTSERSUCHEN UND BESCHWERDEN .....</b>	<b>35</b>
6.1	BEIM SWR EINGEGANGENE AUSKUNFTSERSUCHEN UND BESCHWERDEN .....	35
6.1.1	<i>Direkteingaben zum Rundfunkbeitragseinzug .....</i>	36
6.1.2	<i>Sonstige Direkteingaben beim Rundfunkdatenschutzbeauftragten .....</i>	36
6.2	ANFRAGEN UND AUSKUNFTSERSUCHEN BEIM BEITRAGSSERVICE IN KÖLN .....	37
6.3	AUSBlick ZU AUSKUNFTSERSUCHEN UND BESCHWERDEN .....	37
<b>7</b>	<b>ORGANISATION UND ZUSAMMENARBEIT BEI DER DATENSCHUTZKONTROLLE .....</b>	<b>38</b>
7.1	AUFBAU UND ORGANISATION AUF EUROPÄISCHER EBENE .....	38
7.2	AUFBAU UND ORGANISATION IN DEUTSCHLAND .....	38
7.3	AUFBAU UND ORGANISATION BEI DEN RUNDFUNKDATENSCHUTZBEAUFTRAGTEN .....	39
7.4	ZUSAMMENARBEIT ALLER AUFSICHTSBEHÖRDEN AUF NATIONALER EBENE .....	39
7.5	ZUSAMMENARBEIT DER DATENSCHUTZBEAUFTRAGTEN AUF LÄNDEREBENE.....	41

---

7.6	KONFERENZ UND ARBEITSKREIS DER RUNDFUNKDATENSCHUTZBEAUFTRAGTEN .....	41
<b>8</b>	<b>DER RUNDFUNKBEAUFTRAGTE FÜR DEN DATENSCHUTZ IM SWR.....</b>	<b>43</b>
8.1	RECHTSGRUNDLAGEN .....	43
8.2	STELLUNG DES RUNDFUNKDATENSCHUTZBEAUFTRAGTEN.....	43
8.3	AUFGABEN UND BEFUGNISSE DES RUNDFUNKDATENSCHUTZBEAUFTRAGTEN .....	43
8.4	REGELUNGEN ZUM TÄTIGKEITSBERICHT .....	44
8.5	TATKRÄFTIGE HILFE .....	45
<b>9</b>	<b>ANHANG .....</b>	<b>46</b>
9.1	§ 39 STAATSVERTRAG ÜBER DEN SÜDWESTRUNDFUNK.....	46
9.2	§ 9C RUNDFUNKSTAATSVERTRAG IN DER FASSUNG DES 21. RUNDFUNKÄNDERUNGS-STAATSVERTRAGES; GÜLTIG SEIT 25.05.2018 .....	46
9.3	§ 27 LANDESDATENSCHUTZGESETZ BADEN-WÜRTTEMBERG (LDSG BW) .....	48
9.4	LISTE DER AUFSICHTSBEHÖRDEN NACH ARTIKEL 51 FF. DSGVO ÜBER ARD, ZDF, DW, DLR.....	50
9.5	POSITIONSPAPIER DER RUNDFUNKDATENSCHUTZKONFERENZ (RDSK): .....	51
<b>10</b>	<b>STICHWORTVERZEICHNIS.....</b>	<b>53</b>

## Zusammenfassende Würdigung

Die **Umsetzung der EU-Datenschutzverordnung** vom Mai 2018 ist weder in Europa noch bei den Unternehmen und Behörden und auch nicht beim SWR abgeschlossen. Dies wird noch Jahre dauern und ist abhängig davon, inwieweit man entsprechende Anstrengungen unternehmen will. Ein zentrales Problem in allen Bereichen ist die Frage der **Löschung** nicht mehr benötigter Daten. Unabhängig davon, dass nicht jede Software dazu in der Lage ist, erfordert es organisatorische Anstrengungen, um Löschrufen und Löschroutinen zu erarbeiten und zu prüfen (vgl. auch Ziff. 5.2 des TB).

Auch der SWR hat das **Ziel noch nicht erreicht**. Fast hat man den Eindruck, dass die Umsetzung dem Kontrollorgan und damit dem Rundfunkbeauftragten für den Datenschutz überantwortet wird, anstatt eigenständige Anstrengungen zu unternehmen.

Der vorliegende Tätigkeitsbericht für das Jahr 2019 stellt **im ersten Abschnitt** zunächst die nach wie vor unverminderte **gesetzgeberische Tätigkeit** dar, insbesondere auf europäischer Ebene.

Datenschutzfragen nehmen insbesondere **im Programm und Produktionsbereich** des SWR zu. Die Ausweitung der SWR-Programme im Onlinebereich erhöhen den datenschutzrechtlichen Beratungsbedarf. Es bedarf besonderer Anstrengungen, die Persönlichkeitsrechte der Zuhörer, Zuschauer und Internetnutzer, die immer kritischer werden, zu gewährleisten (**im zweiten Abschnitt**).

Einsparungen und Umstrukturierungen bewirken, dass auch der Datenschutz **im Verwaltungsbereich (dritter Abschnitt)** nicht zur Ruhe kommt. Leider sind immer noch nicht alle Mitarbeiter auf die Vertraulichkeit verpflichtet (vgl. Ziff. 3.1).

Ein **Klassiker** ist dagegen der Datenschutz beim ARD ZDF Deutschlandradio **Beitragsservice**. Erfreulicherweise verursachte der Meldedatenabgleich kaum Probleme (**vierter Abschnitt**).

Keine Entspannung und eine ständige Gefahrenquelle sind – wie **im fünften Abschnitt** ausgeführt - die Angriffe auf die **Datensicherheit** beim SWR (wie auch bei anderen Firmen und Behörden).

Probleme bereiten die immer zahlreicher werdenden und in Umfang und Komplexität (und auch Aggressivität) **steigenden Beschwerden** und Anfragen, insbesondere von Rundfunk-Beitragsteilnehmern (**sechster Abschnitt**).

Die Neustrukturierung der **Datenschutzkontrolle** bei den **öffentlich-rechtlichen Rundfunkanstalten** war auch im Jahr 2019 noch nicht abgeschlossen. Nach wie vor besteht bei der Zusammenarbeit mit den **staatlichen Datenschutzbeauftragten** des Bundes und der Länder noch sehr viel Luft nach oben (**siebter Abschnitt**).

Abgerundet wird der Bericht durch Darstellung des Rundfunkbeauftragten für den Datenschutz im SWR (**achter Abschnitt**).

Stuttgart im Januar 2020

Prof. Dr. Armin Herb

## 1 Entwicklung des Datenschutzrechts im Jahr 2019

Auch wenn die **EU-Datenschutz-Grundverordnung** (DSGVO) bereits zum 25. Mai 2018 in Kraft getreten ist, waren und sind die Einzelheiten der **Umsetzung bis heute offen und umstritten**. In vielen Bereichen gibt es weder eine einheitliche Rechtsauffassung der Aufsichtsbehörden noch eine gesicherte Rechtsprechung. Nicht einmal die in Umsetzung der DSGVO erforderliche Anpassung einer Vielzahl von Bundes- und Landesgesetzen ist abgeschlossen. Nachfolgend wird die neue Rechtsentwicklung dargestellt, soweit sie auch den SWR betrifft:

### 1.1 Europäische Datenschutz-Grundverordnung

Für die Umsetzung der DSGVO ist insbesondere die Arbeit des Europäischen Datenschutzausschusses und die Rechtsprechung des Europäischen Gerichtshofes (EuGH) von Bedeutung.

- Der **Europäische Datenschutzausschuss** (Art. 68 DSGVO) veröffentlicht zwar eine Vielzahl von Papieren (durchweg nur in englischer Sprache), hat es aber bislang nicht geschafft, einheitliche Kriterien z.B. für die Datenschutzfolgenabschätzung zu entwickeln. So hat jede Aufsichtsbehörde eines Mitgliedstaates eigene Regelungen genehmigt bekommen.

Der **Europäische Gerichtshof** (EuGH) nimmt indessen jede Gelegenheit wahr, die Auslegung der DSGVO voranzutreiben. In mehreren Urteilen im Jahre 2019 hat sich der EuGH mit der gemeinsamen Verantwortlichkeit („joint controllers“), der Löschung bei Suchmaschinenbetreibern bzw. Hosting-Anbietern, der Einbindung von Plugins bzw. Gefällt-Buttons, der Einwilligung und Cookies beschäftigt und leistet damit Beiträge zur Auslegung der DSGVO (EuGH vom 29.7.2019, C-40/17; vom 24.9.2019, C-136/17 sowie C-507/17; vom 1.10.2019, C-673/17; vom 3.10.2019, C-18/18).



## **1.2 Weitere europäische Verordnungen und Richtlinien zum Datenschutz**

### **1.2.1 E-Privacy-VO als Nachfolge der RiLi 2002/58 zur elektronischen Kommunikation**

**Gleichzeitig** mit der EU-Datenschutz-Grundverordnung sollte auch eine sogenannte **ePrivacy-Verordnung** veröffentlicht werden. Darauf warten die Rechtsanwender noch heute.

Mit der Verordnung soll insbesondere der Datenschutz bei den Telemedien einschließlich solcher für Trackingverfahren und Cookies geregelt werden, was auch zur Ablösung des Telemediengesetzes (TMG) führen würde. Leider geht die Hängepartie weiter (vgl. auch bereits Ziff. 1.2.2 des 10. Tätigkeitsberichts). Dies ist besonders misslich, weil man sich davon Rechtsklarheit im Hinblick auf Trackingverfahren und Cookies erhofft, einen Bereich, der höchst umstritten ist. Es gibt zwar Regelungen im Telemediengesetz (TMG), aber dieses soll nach Auffassung einiger staatlicher Aufsichtsbehörden gar nicht mehr anwendbar sein, obwohl weder das Bundesverfassungsgericht noch der EuGH die Rechtswidrigkeit des TMG bis heute festgestellt haben.

### **1.2.2 EU-Verordnung zur Cybersicherheit vom 17.4.2019**

Die Verordnung 2019/881 der EU vom 17. April 2019 (ABl. L 151/15 vom 7.6.2019) will das ordnungsgemäße Funktionieren des Binnenmarktes gewährleisten und gleichzeitig ein hohes Niveau in der **Cybersicherheit** und die Fähigkeit zur **Abwehr von Cyberangriffen** erreichen. Dazu werden die Ziele, Aufgaben und organisatorischen Aspekte der „**Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)**“ festgelegt und Festlegungen „**europäischer Schemata für die Cybersicherheitszertifizierung**“ getroffen.

### **1.2.3 EU-Verordnung vom 20. Juni 2019 zu Online-Vermittlungsdiensten**

Auf europäischer Ebene sind nach wie vor verstärkte Aktivitäten im Bereich der gesetzlichen Regulierung der Digitalisierung zu verzeichnen. So gibt es jetzt die **EU-Verordnung** 2019/1150 vom 20. Juni 2019 „zur Förderung von Fairness und Transparenz für gewerbliche **Nutzer von Online-Vermittlungsdiensten**“ (Amtsblatt vom 11. Juli 2019, L 186/57). Damit soll sichergestellt werden, „dass für gewerbliche Nutzer

von Online-Vermittlungsdiensten und Nutzer mit Unternehmenswebsite im Hinblick auf Suchmaschinen eine angemessene Transparenz, Fairness und wirksame Abhilfemöglichkeiten geschaffen werden“ (Art. 1 Abs. 1). Den **SWR** wird man jedoch nicht unter den Begriff des gewerblichen Nutzers fassen können, da weder eine geschäftliche Tätigkeit vorliegt, noch Waren oder Dienstleistungen angeboten werden, zumal der SWR lediglich seinem insbesondere im SWR-Staatsvertrag festgeschriebenen **gesetzlichen Auftrag** nachkommt, „durch die Herstellung und Verbreitung seiner Angebote in Hörfunk, Fernsehen und Internet als Medium und Faktor des Prozesses freier individueller und öffentlicher Meinungsbildung zu wirken und dadurch die demokratischen, sozialen und kulturellen Bedürfnisse der Gesellschaft zu erfüllen“ (Art. 3 Abs. 1 Satz 1 SWR-StV).

#### **1.2.4 EU-Richtlinie zum Schutz von Personen, die Verstöße melden vom 23.10.2019**

Die Europäische Union hat am 23. Oktober 2019 die Richtlinie 2019/1937 „zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“ erlassen (sog. **Whistleblower-RiLi**). Sie wurde am 26.11.2019 im Amtsblatt veröffentlicht (ABl. L 305/17) und muss von den Mitgliedsstaaten bis zum 17. Dezember 2021 in nationales Recht umgesetzt werden.

Die Vorschrift bezweckt den **Schutz von Hinweisgebern** (Whistleblower bzw. Informanten). Dazu werden die Mitgliedstaaten verpflichtet, entsprechende gesetzliche Bestimmungen zu schaffen. Die Richtlinie fordert zunächst Regelungen bei **Verstößen gegen das Unionsrecht** (Art. 1). Dazu wird in einer umfangreichen Anlage aufgeschlüsselt, welche Richtlinien und Verordnungen der EU darunterfallen. Wie sich aus dem Erwägungsgrund 14 ergibt, wird die Meldung von Hinweisgebern als besonders nützlich angesehen, wenn dadurch Sicherheitsvorfälle oder **Verstöße gegen die Datenschutzvorschriften der EU** verhindert werden. Deshalb sollen beispielsweise auch Hinweise von Informanten im Hinblick auf die Datenschutz-Grundverordnung sowie die Richtlinie für die elektronische Kommunikation oder diejenige zur Gewährleistung der Netz- und Informationssicherheit in der EU durch die Vorschrift geschützt werden (vergleiche Ziff. J des Anhangs, Teil I – L 305/55).

Die Richtlinie lässt aber die Befugnis der Mitgliedstaaten unberührt, den Schutz auf andere Bereiche der Rechtsakte auszudehnen (Art. 2 Abs. 2). Es wird sich zeigen, wie schnell der deutsche Gesetzgeber diese Richtlinie zum Schutz von Hinweisgebern umsetzt und eine **Harmonisierung** mit dem gerade erst erlassenen **Geschäftsgeheimnisgesetz** (siehe nachfolgend Ziff. 1.3.2) vornimmt.

### 1.3 Gesetzgebung im Bereich des Bundes

#### 1.3.1 Bundesdatenschutzgesetz II vom 20.11.2019

Die Anpassung deutscher Gesetze an die EU-Datenschutz-Grundverordnung wurde mit dem „**Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU**“ vom **20. November 2019** fortgesetzt. Es ist im Gesetzblatt Nr. 41 vom 25.11.2019 als Art. 12 veröffentlicht worden (BGBl. I 2019, S.1626, 1633 f.). Neben 154 Fachgesetzen (z.B. als Art. 41 das Deutsche-Welle-Gesetz) wurde auch wieder das **BDSG geändert** und zwar in folgenden Punkten:

- Die Schwelle zur **Bestellung eines betrieblichen Datenschutzbeauftragten** wurde in § 38 BDSG von zehn auf zwanzig Personen erhöht. Dies ändert aber nichts daran, dass nach wie vor eine Fülle von datenschutzrechtlichen Pflichten auch für kleine Unternehmen (oder auch z.B. Vereine) besteht.
- Die **Aufsichtsbefugnisse des Bundesdatenschutzbeauftragten (BfDI)** wurden nicht nur gestärkt (z.B. im Hinblick auf Unternehmen, die Telekommunikationsdienstleistungen erbringen), sondern auch überflüssigerweise auf den Verwaltungsbereich der **Deutschen Welle** ausgedehnt (§ 65 Deutsche-Welle-Gesetz in der Fassung vom 20. November 2019, BGBl. 2019, S. 1650 f.).
- Mit einer Änderung des § 22 BDSG soll eine **Weitergabe sensibler Informationen** „im Rahmen von Präventions- und Deradikalisierungsprogrammen“ an „Sicherheitsbehörden“ ermöglicht werden.
- Beim **Beschäftigten-Datenschutz** (§ 26 BDSG) ist jetzt festgehalten, dass die **Einwilligung** zukünftig auch **elektronisch** erfolgen kann.
- Schließlich wird die Zulässigkeit der Verarbeitung von Daten zu Zwecken staatlicher **Auszeichnungen und Ehrungen** durch einen neuen § 86 BDSG geregelt.

### **1.3.2 Gesetz zum Schutz von Geschäftsgeheimnissen vom 18.4.2019**

Der Bundestag hat am 18. April 2019 das Gesetz „zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung“ erlassen (BGBl. 2019, S. 466 ff.). Damit sollte die **EU-Richtlinie** 2016/943 vom 8. Juni 2016 „über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (**Geschäftsgeheimnisse**)“ umgesetzt werden (ABl. 2016 vom 15.6.2016, L 157/1). Jetzt gibt es aber eine neue Richtlinie 2019/1937 „zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“ (sog. Whistleblower-RiLi; siehe oben Ziff. 1.2.4), womit wohl eine erneute Anpassung und Harmonisierung dieses Gesetzes (bis zum 17. Dezember 2021) erfolgen muss.

### **1.3.3 Gesetz des Bundes zur Kontrolle von Diesel-Fahrverboten vom 8.4.2019**

In viele Städte darf mit bestimmten Typen von **Dieselfahrzeugen** nicht mehr gefahren werden. Dies betrifft nicht nur Mitarbeiter des SWR, sondern auch **Dienstfahrzeuge** wie Übertragungswagen (sofern keine Ausnahmegenehmigung möglich ist). Um das Verbot zu kontrollieren, wurde am 8. April 2019 das Straßenverkehrsgesetz geändert (BGBl. 2019, Seite 430); auf einen entsprechenden Entwurf hatte ich bereits im letzten 11. Tätigkeitsbericht unter Ziff. 1.3.4 hingewiesen. Die Bundesregierung will durch Änderung des Straßenverkehrsgesetzes **Kamerabilder von allen Fahrzeugen** erstellen, gleich ob mit Diesel betrieben oder nicht. Auf den Bildern sollen Nummernschild, Fahrer und weitere Fahrzeugmerkmale zu sehen sein. Die erfassten Daten werden dann automatisch mit dem Fahrzeugregister des Kraftfahrt-Bundesamtes abgeglichen. Nachdem der Bundesrat einen ersten Entwurf abgelehnt hatte (BRat-Drs. 574/1/18), wurde nun eine Entschärfung der datenschutzrechtlichen Regelungen vorgenommen. Eine verdeckte Datenerhebung ist jetzt unzulässig, es darf nur eine stichprobenartige Überprüfung erfolgen und die Lösungsfristen wurden gekürzt. Das Gesetz ist im Bundesgesetzblatt 2019 Seite 430 f. abgedruckt.

### **1.3.4 Gesetzentwurf zu Abmahnverfahren**

Die Bundesregierung hat am 31. Juli 2019 den Entwurf eines „**Gesetzes zur Stärkung des fairen Wettbewerbs**“ in den Bundestag eingebracht (BTags-Drucksache 19/12084).

Ziel sei die Vermeidung von missbräuchlichen Abmahnungen, insbesondere auch im Bereich des Datenschutzes. Der Gesetzentwurf hat weitere umfangreiche gesetzgeberische Initiativen ausgelöst und wurde am 26. September 2019 vom Bundestag in die Ausschüsse verwiesen.

#### **1.4 Gesetzgebung im Bereich der Zuständigkeit der Länder**

Auch im Bereich der Zuständigkeit der **Länder** mussten die Gesetze mit Datenschutzregelungen an die EU-Datenschutz-Grundverordnung angepasst werden. Deshalb wurden nicht nur alle (allgemeinen) **Landesdatenschutzgesetze angepasst** und die bereichsspezifischen Gesetze geändert, sondern auch entsprechende Staatsverträge zwischen den Ländern (z.B. im Rundfunkbereich).

Die **Änderung des Landesdatenschutzgesetzes Baden-Württemberg** durch Art. 3 des Finanzausgleichsgesetzes vom 18. Dezember 2018 ließ § 27 LDSG BW unberührt und **erhöhte** lediglich in § 23 LDSG BW die **Besoldung des Landesdatenschutzbeauftragten** von B5 auf B6 (GBl. BW 2019, 1549, 1551). Die Vergütung des **Rundfunkbeauftragten** für den Datenschutz beim **SWR** (vgl. § 27 Abs. 3 Satz 2 LDSG BW) wurde durch den SWR-Verwaltungsrat **nicht geändert**.

##### **1.4.1 Rundfunkstaatsverträge**

Im **Bereich des Rundfunkwesens** handeln die Länder dadurch, dass sie **Staatsverträge** abschließen, die dann von den Landesparlamenten in das jeweilige Landesrecht umgesetzt werden.

- Durch den **22. Rundfunkänderungsstaatsvertrag** wurde der Rundfunkstaatsvertrag (RStV) mit Wirkung zum 1. Mai 2019 geändert (GBl. BW 2019, Seite 27 ff.). Dort wurden insbesondere die **Regelungen für die Telemedien** der Rundfunkanstalten **geändert**.
- Der **23. Rundfunkänderungsstaatsvertrag** wurde Ende Oktober 2019 unterzeichnet und soll nach Ratifizierung durch die Landesparlamente am 1. Juni 2020 in Kraft treten (vgl. LTags-Drs. BW 16/6539). Der

Rundfunkbeitragsstaatsvertrag würde damit in einigen Punkten geändert werden: Zunächst werden die Vorgaben des Bundesverfassungsgerichts zur Befreiung von Zweitwohnungen umgesetzt (vgl. näher Ziff. 1.4.4 des 11. TB 2018). Des Weiteren soll der **Melddatendatenabgleich** mit dem Bestand der Rundfunkbeitragsteilnehmer **zukünftig regelmäßig** (nach Prüfung durch die KEF) stattfinden (vgl. dazu auch Ziff. 1.4.3 des 11. TB). Schließlich wurden weitere Anpassungen an die DSGVO vorgenommen: Dies betrifft vor allem Auskunftsrechte und Informationspflichten, die Sicherstellung geeigneter technischer und organisatorischer Maßnahmen sowie eine Rechtsgrundlage für den Erlass automatisierter Beitragsbescheide durch den Beitragsservice.

#### **1.4.2 Rundfunkfinanzierungs-Staatsvertrag**

**Keine Änderung** erfuhr der **Rundfunkfinanzierungs-Staatsvertrag**, obwohl auch hier dringend eine Anpassung notwendig wäre. Denn nach wie vor fehlt der **Kommission zur Ermittlung des Finanzbedarfs (KEF)** eine **Rechtsgrundlage** zur Erhebung und Verarbeitung **personenbezogener** Daten (vgl. schon Ziff. 1.4.2 und Ziff. 3.11 des 10. Tätigkeitsberichts sowie Ziff. 1.4.2 des 11. TB).

#### **1.5 Datenschutzrichtlinie des Europarates (Konvention 108)**

Der **Europarat** hat bereits 1981 das internationale „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ (Konvention 108) verabschiedet. Inzwischen wurde ein modernisiertes Abkommen abgeschlossen und wartet auf die Ratifizierung durch die Staaten.

## 2 Datenschutz im Programm- und Produktionsbereich des SWR

### 2.1 TikTok – der 15-Sekunden-Wahn bei Jugendlichen

**TikTok** ist die App eines Dienstleisters für Smartphones. Man kann damit kurze (meist 15 Sekunden lange) **Clips aufnehmen** und diese zudem schnell bearbeiten. Von den meist nur zwischen 14 und 20 Jahre alten Nutzern (oder noch jünger) wurde sie weltweit bislang mehr als 1,5 Milliarden Mal heruntergeladen. Seit kurzem ist auch die **Tagesschau auf TikTok** mit einem Account vertreten, um Nachrichten einer jüngeren Zielgruppe nahe zu bringen. *Funk* ist bereits mit fünf Formaten präsent. Dabei ist TikTok nicht nur bei Datenschützern umstritten. Diese chinesische Kurzvideoplattform der **Firma ByteDance** steht in der Kritik, Inhalte zu zensieren und ist im Verdacht, Algorithmen zur Gesichtserkennung für die chinesischen Behörden zu trainieren. Erst kürzlich berichtete die Tagesschau über das Geschäftsgebaren des Unternehmens, politische Videos zu filtern. Dagegen stört sich ByteDance offenbar kaum daran, dass meist junge Mädchen in tausenden Videos ihre zerbrechlichen Körper in einer Magersucht-Challenge zur Schau stellen.

Wie viele andere Dienstleister „kostenloser Software“ gibt auch ByteDance Daten an Dritte weiter, um dem Nutzer auf seine Bedürfnisse zugeschnittene Angebote, sprich Werbung, zu unterbreiten. Dafür kennt die **Sammelwut der App** keine Grenzen: TikTok erhebt gemäß seiner Datenschutzerklärung neben den Kontaktdaten seiner Nutzer auch technische Daten, IP-Adresse, Browserverlauf, Mobilfunkanbieter, Nutzungsdaten sowie Kommunikationspräferenzen, Nachrichteninhalte mit Empfänger, aber auch Daten anderer sozialer Netzwerke wie z.B. Login-Daten. TikTok sammelt die Daten aber nicht nur zu Werbezwecken. So gehen auch Daten an Google, das **zu Analyse Zwecken Google Analytics** einsetzt. Kürzlich hat der Bundesbeauftragte für den Datenschutz in einer Presseerklärung vom 14.11.2019 klargestellt, dass personenbezogenes Webtracking nur mit **datenschutzkonformer Einwilligung** möglich sei. ByteDance stellt den Nutzern von TikTok zwar eine Möglichkeit zum Abmelden solcher Datenerhebungen zur Verfügung. Eine **Opt-Out Funktion** kann jedoch keine Einwilligung ersetzen.

Doch auch falls ByteDance Tracking nur mittels Einwilligung der Nutzer durchführen ließe, könnten **Minderjährige** unter 16 Jahren nicht wirksam in die Erhebung Ihrer Daten einwilligen. Zu ihrem Schutz sieht die DSGVO die **Einwilligung der Eltern** vor.

Vermutlich ist die Nutzung von TikTok daher erst ab dreizehn Jahren und auch nur mit Einwilligung der Eltern erlaubt. Sofern dies aber nicht kontrolliert wird und eine falsche Angabe des Alters möglich bleibt, ist der besondere Schutz von Minderjährigen nicht gewährleistet. Aus allen vorgenannten Gründen sehe ich den Einsatz von TikTok daher kritisch.

## 2.2 *WhatsApp*

Der Messenger Dienst WhatsApp ist immer wieder in der Diskussion. Mehr oder minder regelmäßig erreichen mich Beschwerden, dass der SWR auf WhatsApp als Kommunikationskanal hinweist. Solange allerdings WhatsApp nur als eine von vielen **Möglichkeiten der Kommunikation** angeboten wird, ist dagegen aus Gründen des Wettbewerbsschutzes und Diskriminierungsverbotes nichts einzuwenden. Fraglich ist aber in der Tat, ob WhatsApp trotz seiner datenschutzrechtlich problematischen Ausrichtung wirklich eingesetzt werden soll.

... und dann noch: **Whats up?**

Im Berichtszeitraum erreichte mich die Beschwerde eines Hörers, der sich mit einem Anliegen in einem Chat an SWR3 über den bekannten Messenger Dienst WhatsApp gewandt hatte. In seinen Kurznachrichten zeichnete der Hörer immer mit seinem Vornamen. Die Redaktion antwortete ihm darauf unter Nutzung seines vollständigen Namens. Nach Rücksprache mit der Redaktion erhielt ich die Rückmeldung, dass das Studiofeedback-System anders funktioniert als die App auf dem Smartphone. In dem Studiofeedback-System werden keine Kontakte gespeichert. Vielmehr zeigt das Feedback-System der Redaktion immer den Namen an, der von den Geräten des Hörers an das SWR-System übermittelt wird. Sobald die Redaktion auf eine Nachricht antwortet, erscheint automatisch die Anrede mit dem Namen des Hörers. Und dies ist der Name, der in den Einstellungen von WhatsApp hinterlegt ist. Man findet seine eigene WhatsApp-Kennung unter „Einstellungen“ mit dem Hinweis „Dieser Name wird für deine WhatsApp Kontakte sichtbar sein“. Das kann der Vorname, der vollständige Name oder auch ein Spitzname sein.



### **2.3 Twitter abgeschaltet**

Der Landesdatenschutzbeauftragte von Baden-Württemberg, Dr. Stefan Brink, hat zum Ende des Jahres 2019 angekündigt, seinen **Twitter-Account abzuschalten**. Seine Begründung: **Twitter erhebe im Hintergrund Nutzerdaten** und sei ein datenschutzrechtlich problematisches Netzwerk. Der rheinland-pfälzische Landesdatenschutzbeauftragte, Prof. Dr. Dieter Kugelmann rät Behörden, Seiten auf Twitter und **Facebook abzuschalten**.

Auch beim SWR wird Twitter eingesetzt. Der **SWR nutzt** neben **Twitter** auch andere soziale Medien wie **Facebook, Instagram oder flickr**. Die Begründung für alle diese Dienste ist, dass der SWR den Auftrag habe, die gesamte Bevölkerung zu erreichen und damit alle Generationen und Gruppen auf ihren jeweiligen sozialen Plattformen erreichen müsse. Auf der anderen Seite muss berücksichtigt werden, dass der SWR damit seine Hörer und Seher auf datenschutzrechtlich bedenkliche Plattformen und Dienste lockt.

### **2.4 Ärger um ScribbleLive**

In meinem vorletzten Tätigkeitsbericht (10. TB) habe ich bereits über Probleme mit **ScribbleLive** berichtet. Mit diesem Werkzeug werden Informationen (vorwiegend aus sozialen Netzwerken) ausgewählt, zusammengestellt und aufbereitet. Dies ist im Grundsatz nichts anderes als Redaktionsarbeit, läuft aber unter dem Begriff „**kuratieren**“. Nun gab es erneut eine Datenschutzbeschwerde über das Kuratierungstool des Content-Cloud-Anbieters, die von einem Beschwerdeführer beim rbb und auch beim hr einging. Darin wurde vorgebracht, dass beim Aufruf von Seiten der Rundfunkanstalten automatisch Verbindungen zu Drittservern hergestellt werden.

Und tatsächlich hat eine Überprüfung durch den rbb den Abfluss von Daten ergeben. So wurden durch das Einbinden von Drittinhalten beispielsweise aus Youtube, Facebook, Twitter oder Instagram Nutzerdaten entgegen vertraglicher Zusicherungen übermittelt. Daraufhin haben die betroffenen Rundfunkanstalten umgehend reagiert und vorübergehend auf eine **Zwei-Klick-Lösung** umgestellt. Zudem wurde ScribbleLive über den Missstand informiert. Der Anbieter reagierte mit dem Vorschlag, den bereits bei Youtube und Twitter praktizierten **Privacy-Enhanced-Modus**, also eine datenschutzfreundliche Lösung, einzusetzen. Da der SWR für ARD-Online und auch in

Sachen ScribbleLive innerhalb der ARD federführend ist, wurde ich von den Kollegen um eine datenschutzrechtliche Bewertung gebeten.

Der Privacy-Enhanced-Modus zielt darauf ab, Fremdinhalte anbieten zu können, ohne automatisch Daten an die jeweiligen Anbieter zu übermitteln. Erst wenn beispielsweise ein eingebundenes Video im Tool angeklickt wird, findet ein Datenaustausch mit der verantwortlichen Social-Media-Plattform statt. Doch allein in dem Abrufen der Inhalte kann **keine wirksame Einwilligung** der Nutzer gesehen werden, freiwillig personenbezogene Daten an Dritte zu übermitteln. Vielmehr bedarf es einer Einwilligung, die voraussetzt, dass die Nutzer umfassend informiert sind, um die Tragweite ihrer Handlung erkennen zu können. Dementsprechend habe ich in enger Zusammenarbeit mit der Entwicklung von ARD-Online einen modifizierten Vorschlag ausgearbeitet.

Erfreulicherweise hat ScribbleLive unsere Anregungen aufgegriffen und entwickelt nun für die ARD eine technische Lösung zur Einbindung einer Information zum Datenschutz. Diese Information soll den Nutzern im Frontend, also auf dem Bildschirm, in der Form angezeigt werden, dass auf die Einbindung von Drittinhalten verwiesen wird. Die Inhalte können erst abgerufen werden, wenn der Nutzer ausdrücklich zustimmt.

## **2.5 SWR3 pushed**

Zum Jahresanfang 2019 hat SWR3 als erstes Portal in der ARD Website-Pushes eingeführt. Dabei handelt es sich um Mitteilungen, die der Besucher der Website nicht eigenständig aufrufen muss. **Push-Mitteilungen** öffnen sich automatisch, bei Verwendung in einer App auch auf dem Smartphone. Dies allerdings nur, sofern der Nutzer grundsätzlich zugestimmt hat, solche Nachrichten zu erhalten. Zudem kann der Nutzer auswählen, zu welchen Themen Push-Mitteilungen gesendet werden sollen.

Um **Push-Mitteilungen datenschutzkonform** einzubinden, ist es notwendig, die Datenschutzerklärung des Onlineangebots anzupassen. Der Nutzer muss über die Verarbeitung seiner personenbezogenen Daten informiert sein, insbesondere auf welcher Rechtsgrundlage dies geschieht. Auch auf die Speicherdauer bzw. Löschung der Daten ist einzugehen. Da für den Bezug der Push-Mitteilungen eine Einwilligung des Nutzers erforderlich ist, muss auf das **Widerrufsrecht** hingewiesen werden. Die Ausübung des Widerrufsrechts ist dem Nutzer so einfach wie möglich zu machen, indem

im Zusammenhang mit dem Hinweis auf das Widerrufsrecht eine Mailadresse zu nennen ist, an die der Nutzer seinen Widerruf senden kann. Nach kurzem Austausch mit der Redaktion von SWR3 wurde die Datenschutzerklärung unter den genannten Gesichtspunkten ergänzt und unter dem klarstellenden Hinweis angepasst, dass eine Weitergabe von Daten ausgeschlossen ist.

## **2.6 Onsite-Befragung bei SWR 3**

Als erste Marke in der ARD plante SWR 3 eine dauerhafte Onsite-Umfrage auf deren Website, die zudem in der Lage sein sollte, möglichst hohe Datenschutzstandards zu setzen. Bei einer **Onsite-Befragung** handelt es sich um eine **Form der Online-Befragung**, die der Verbesserung der Nutzerfreundlichkeit dient. Dafür wird bei einer bestimmten Anzahl an Besuchern der Website ein Flash-Layer eingeblendet, der auf die Umfrage hinweist.

So sollte auf den Seiten von SWR 3 einem kleinen Kreis jeden Tag zufällig drei Fragen aus einem größeren Pool zu Radio- oder Onlineinhalten gestellt werden. Die Fragen für die Umfrage wurden vorab mit Questback, einem Dienstleister, erstellt. Wichtig war mir dabei vor allen Dingen, dass die Transparenz gegenüber den Teilnehmern gewahrt wird. Die Beantwortung der Fragen musste freiwillig sein und es durften keinerlei personenbezogene Daten gespeichert werden. Dementsprechend ist zum Beispiel die Angabe von Geschlecht und Geburtsjahr optional und die Umfrage völlig anonym. Die notwendigen Datenschutzinformationen erhält der Nutzer dann über eine verlinkte Datenschutzerklärung. Mit der Möglichkeit zum frühzeitigen Abbruch erhält der Teilnehmer zudem auch die Möglichkeit, von seinem Widerspruchsrecht Gebrauch zu machen. Letztlich habe ich der dauerhaften Onsite-Umfrage zustimmen können, da zudem durch die vorbildlich geringe Anzahl der anonym durchgeführten Fragen eine Profilbildung von vornherein ausgeschlossen ist.

## **2.7 Die Webcam am Bodensee**

Das Studio Friedrichshafen hat eine Webcam mit Blick auf den Bodensee und die Berge. Nach Inkrafttreten der Datenschutz-Grundverordnung kamen Zweifel auf, ob die Webcam noch zulässig ist. Dies beurteilt sich danach, welche Bilder zu sehen sind. Die Webcam erfasste einen Teil eines Fahrradweges sowie Bänke im Vordergrund. Personen, die sich in diesem Bereich aufhielten, waren damit identifizierbar. Somit lagen

personenbezogene Daten vor, wodurch nicht nur die Regelungen der DSGVO gelten, sondern auch § 18 Landesdatenschutz Baden-Württemberg. Danach ist eine Webcam, also Videoüberwachung, nur zulässig zur Ausübung des Hausrechts oder zur Aufgabenerfüllung. Da es zu den Aufgaben des SWR gehört, Sendungen zu verbreiten, nicht aber eine Webcam aufzustellen, musste die Webcam des Studios Friedrichshafen so umgestellt werden, dass keine Personen mehr zu identifizieren sind. Jetzt wurde sie so eingerichtet, dass nur noch im unteren Bildrand Bäume, dann der Bodensee und im Hintergrund die Berge zu sehen sind (sofern der Nebel nicht die Sicht versperrt).

## **2.8 Viel Lärm um den Datenschutz**

Im letzten Berichtszeitraum hatten einige Mitarbeiter im Zuge der Verpflichtung auf die Vertraulichkeit Kritik über die Ihnen zur Verfügung gestellten Mittel geäußert, um beispielsweise Akten datenschutzkonform vernichten zu können. Dieses Thema habe ich aufgegriffen und unter anderem beim Studio Tübingen nachgefragt, wie es dort um die Aktenvernichtung bestellt ist. Ein Aktenvernichter macht vor allem dann Sinn, wenn er zentral aufgestellt wird und allen Mitarbeitern zugänglich ist. Idealerweise bietet sich dafür ein Platz in der Nähe von Druckern an, auch um Fehldrucke umgehend vernichten zu können.

Im **Studio Tübingen** gab es zwar einen allgemein zugänglichen Aktenvernichter. Dabei handelte es sich aber um ein älteres Modell, das aufgrund seiner Lautstärke in einem separaten Lagerraum untergebracht werden musste. So war es aufgrund seiner Abgeschlossenheit nicht nur umständlich den Aktenvernichter zu benutzen, einige Mitarbeiter wussten auch nicht um diese Möglichkeit. Inzwischen wurden erfreulicherweise vier neue Aktenvernichter angeschafft, die neben den Druckern nun bestens aufgestellt sind. So werden die Aktenvernichter auch genutzt; das ist vorbildlich.

## **2.9 Warnung vor Trickbetrug**

Anfang des Jahres erreichte mich die Beschwerde eines Hörers der ARD Pop Nacht mit der Bitte um Stellungnahme. Der Hörer hatte eine E-Mail ins Studio geschickt, in der er anständigerweise andere Autofahrer vor einem Trickbetrüger warnte, der an der A 3 sein Unwesen trieb. Dabei hatte der Hörer seine personenbezogenen Daten angegeben. In der ARD Pop Nacht wurde die Meldung zu dem Trickbetrüger gesendet und auf den Hörer mit Nennung des Namens und Wohnorts Bezug genommen. Infolgedessen sah sich der

Hörer in seinen Persönlichkeitsrechten verletzt und befürchtete, dass Einbrecher die Gelegenheit nutzen könnten, in sein Haus einzubrechen. Die Befürchtung rührte vor allen Dingen aus dem Umstand, dass er vor „kriminellen Subjekten“ gewarnt hat.

Der SWR nutzt mittlerweile seit vierzig Jahren in seinen Wellen die von Hörern in Sendungen eingebrachten Beiträge, seien es Textmeldungen oder Anrufe. Dabei wird in jedem Fall einzeln abgewogen, ob beim Vorlesen einer Nachricht insbesondere Datenschutz- oder Persönlichkeitsrechte verletzt werden könnten. Die Redakteure prüfen durchweg sehr gewissenhaft, ob eine Inhalts- oder Namensnennung auf den Sender stattfinden kann. In der Regel kann aber ohne Angabe der Quelle kein Beitrag gesendet werden. Auch wenn es sich über diesen Zeitraum um die erste Beschwerde handelt, wird zukünftig in den Eingabefeldern und Datenschutzerklärungen darauf hingewiesen, dass in den Beiträgen eine Nennung mit Namen und Ort erfolgen kann. Der Veröffentlichung kann jedoch widersprochen werden. Selbstverständlich kommt es auch weiterhin zu einer sorgfältigen Prüfung jedes Einzelfalls.

### **2.10 Medialoopster für funk**

Aus dem Bereich Information, Dokumentation und Archive des SWR erhielt ich eine Anfrage zur Prüfung der Software Medialoopster. Bei Medialoopster handelt es sich um eine browserbasierte MAM-Software (SaaS), wobei MAM für Media Asset Management steht. Es geht um die **Verwaltung großer Datenmengen in Form von Videoinhalten**, die im Rahmen des Projektes „Archivierung von Online-Inhalten von *funk*“ notwendig wird. Das System dient der Verwaltung der Originalfiles.

SaaS-Systeme sind in der Handhabung praktisch, da keine Installation der Software auf den eigenen Systemen erfolgen muss. Bei webbasierten Anwendungen kommt es aber in der Regel zum Austausch von Daten. Daher muss immer eine Prüfung erfolgen, ob personenbezogene Daten an den Betreiber der Software übermittelt werden. Um Medialoopster nutzen zu können, ist eine Legitimation in der Anmeldemaske nötig. Die Mitarbeiter müssen sich mit Benutzernamen und Passwort anmelden. Eine Auftragsverarbeitung im Sinne der DSGVO, die den Abschluss eines entsprechenden Vertrages nach Artikel 28 DSGVO notwendig machen würde, ist darin aber nicht zu sehen.

Die Frage, ob Daten beim Einsatz der Software an die Betreiberfirma fließen, stellt sich nicht nur bei den Log-Daten. Auch die Video-Daten können personenbezogene Daten enthalten. Der Schutzbedarf ist jedoch nicht gleichermaßen gegeben, da die Inhalte bereits in diversen Social-Media-Kanälen veröffentlicht wurden. Immerhin handelt es sich dabei jedoch auch um Daten, die unter das Medienprivileg fallen. Bei der Nutzung von Medialoopster werden sowohl die Metadaten als auch die Log-Daten auf einer Datenbank gespeichert, auf die der SWR über eine Schnittstelle den alleinigen Zugriff erhält. Die Videodaten werden in der Folge auf SWR-interne Speicher geschrieben und auf Tapes gesichert. Trotz allem habe ich mich für den Abschluss einer Vertraulichkeitsvereinbarung ausgesprochen, die der SWR vor dem Austausch der Daten mit der Betreiberfirma geschlossen hat.

### **2.11 EVA und der Datenschutz**

EVA ist eine webbasierte **Eventanwendung für Produktions- und Eventplaner**, die der SWR selbst entwickelt hat. Dies auch mit dem Ziel, die Software anderen Anstalten innerhalb der ARD als Betreiber zur Verfügung stellen zu können. So wird EVA künftig ebenfalls vom WDR, NDR und BR eingesetzt. Ein Zugriff auf die Webanwendung ist allerdings nur aus dem ARD-Netzwerk möglich und findet getrennt nach Event und Landesrundfunkanstalt über Benutzerberechtigungen statt. Der Produktionsleiter eines Events wird hierbei zum Eventorganisator, der weitere Sachbearbeiter berechtigt und unterschiedliche Rollen mit verschiedenen Bearbeitungsrechten festlegt.

Für einen datenschutzkonformen Einsatz der Software sind die Anforderungen der DSGVO zu beachten. Denn im Rahmen ihres Dienstverhältnisses werden die Mitarbeiter dazu angehalten, neben reiserelevanten und dienstlichen Daten auch private Daten in die Masken der Software einzugeben. Von besonderem Interesse war dabei, welche Art privater Daten als Pflichtangaben erhoben werden dürfen, um sich beispielsweise bei der Frauenfußball-WM in Frankreich erfolgreich akkreditieren zu können. Wie immer gilt im Datenschutz der Grundsatz der Datenminimierung, wonach die Datenerhebung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Aber nicht nur die **FIFA**, auch die **Deutsche Fußball Liga (DFL)** forderte in der Vergangenheit immer wieder **private Anschriften und Geburtsdaten** von Rundfunkjournalisten und begründete dies mit Sicherheitsinteressen. Es bestünde die Notwendigkeit, diese Daten

für mögliche Anfragen von Sicherheitsbehörden bereit zu halten. Dieser rechtswidrigen Praxis ist nun erfreulicherweise eine Absage erteilt worden.

Zum einen konnte durch Hinweis des Vorsitzenden des AKDSB auf diese unzulässige Datenerhebung der Hessische Beauftragte für Datenschutz und Informationsfreiheit die seiner Aufsicht unterstehende DFL auffordern, die bisherige Praxis zu ändern und die bereits erhobenen Daten zu löschen. Mit der Folge, dass das Unternehmen dazu angehalten ist, datenschutzkonforme Alternativen zu prüfen und eine rechtmäßige Lösung zu finden. Zum anderen stufte der EU-Datenschutzbeauftragte die Erfassung privater Journalistendaten als unrechtmäßig ein. Dessen Stellungnahme bezog sich auf einen Kongress der rechtspopulistischen ENF-Fraktion (eine bis 2019 existierende rechtsorientierte Fraktion im Europäischen Parlament), bei dem auch einigen Journalisten der ARD und des ZDF die Teilnahme verwehrt wurde. Angeblich machten es die hohen Sicherheitsvorkehrungen des Kongresses notwendig, die kompletten Presseausweise mit Privatanschrift dem Veranstalter online zur Verfügung zu stellen. In einer solchen Vorgehensweise sieht der Europäische Datenschutzbeauftragte zu Recht einen Verstoß gegen EU-Recht.

### **2.12 „Applaus für @SWRpresse und funk“**

Zum Ende des Berichtszeitraums erhielt ich die Beschwerde eines Nutzers, der gemeinsam mit einer weiteren Person eine Mail an die Redaktion von *funk*, dem Online-Medienangebot von ARD und ZDF, geschrieben und in diesem Zusammenhang einen DMARC-Hinweis (**D**omain-based **M**essage **A**uthentication, **R**eporting and **C**onformance) von Google erhalten hat. Den Hinweis hat der Beschwerdeführer bekommen, da er DMARC nicht eingerichtet und seine Daten offenbar durch Google verarbeitet worden sind. Dabei ist dem Beschwerdeführer erfreulicherweise aufgefallen, dass nicht *funk* seine Daten an Google weitergegeben hat, sondern die andere Person einen Mailserver von Google nutzte.

Letztlich sind beim Beschwerdeführer aber doch einige Fragen in der Zuständigkeit für den Datenschutz bei *funk* offengeblieben, insbesondere da der Bayrische Rundfunk für EinsPlus verantwortlich sei und vermutlich deren Mailserver genutzt werde, der SWR in der Datenschutzerklärung von *funk* aber als Verantwortlicher genannt wird. Ich klärte daraufhin auf, dass das Programm von EinsPlus bereits im September 2016 eingestellt

wurde. Dafür gibt es *funk*, ein Angebot von ARD und ZDF. In diesem Senderverbund werden Aufgaben zwischen einzelnen Rundfunkanstalten aufgeteilt. Daher ist der SWR beispielsweise für die ARD bei *funk* federführend. Im Rahmen der Aufgabenteilung können auch andere Mailserver des Verbundes genutzt werden.

Der Beschwerdeführer formulierte daraufhin in höflicher Weise den Wunsch nach mehr Transparenz in der Datenschutzerklärung von *funk*. Es sollte für den Nutzer klar erkennbar sein, dass *funk* als Gemeinschaftsprojekt der öffentlich-rechtlichen Rundfunkanstalten auch Dienste anderer Anstalten des Senderverbundes nutzen könne. Diesen Wunsch habe ich gerne umgehend aufgegriffen, so dass in guter Zusammenarbeit mit *funk* eine entsprechende **Anpassung der Datenschutzerklärung** erfolgt ist. Prompt kam dann auch die Rückmeldung des Nutzers auf Twitter „so geht Umgang mit Feedback und #Datenschutz“. Der Nutzer lobte in seiner Mail zudem, dass seine Anregungen ernst genommen und schnell umgesetzt wurden. Es gebe ihm „viel Vertrauen in die Öffentlich/Rechtlichen“.

### **2.13 Umfragen – was gilt es zu beachten?**

In der Wirtschaft werden regelmäßig Umfragen durchgeführt, um zu sehen, ob die Angebote dem Wunsch des Kunden entsprechen. Auch wenn damit in erster Linie der Gewinn gesteigert werden soll, spielen Kundenbindung und Produktoptimierung eine wesentliche Rolle. Beim **öffentlich-rechtlichen Rundfunk** geht es dagegen nicht um Profit, sondern darum, ob und in welchem Umfang das Programm auf den verschiedensten Ausspielwegen Anklang findet. Umfragen kommen aber nicht nur im Programm zum Einsatz. Zu Befragungen kommt es auch zum Mittagessen in der Kantine oder in Bachelor- oder Masterarbeiten von Studenten.

Allen Umfragen ist gemein, dass es zur Erhebung personenbezogener Daten kommt. Bei einem solchen Vorgang sieht die DSGVO eine **Informationspflicht des Verantwortlichen** nach Artikel 13 DSGVO vor. Dafür stelle ich den Fachabteilungen regelmäßig ein Muster zur Verfügung, das die gesetzlichen Anforderungen aufgreift. Sofern bei der Erhebung der Daten ein Dienstleister eingesetzt wird und es zu einer Verarbeitung im Auftrag des SWR durch den Dienstleister kommt, muss ein Auftragsverarbeitungsvertrag (AV-Vertrag) geschlossen werden.



In der Umfrage ist dann darauf zu achten, dass möglichst wenig personenbezogene Daten abgefragt werden. Es gilt das **Prinzip der Datenminimierung**, wonach die Erhebung von Daten auf das notwendige Maß beschränkt sein muss. So ist in Umfragen beispielsweise immer nach Altersspannen und nicht nach dem genauen Alter zu fragen. Auch darf nicht nach der vollständigen Postleitzahl gefragt werden, sondern nur nach den ersten drei Ziffern. Es gilt, bei den nötigen Angaben der Umfrage einen **Personenbezug auszuschließen**. Denn auch mit diesen Einschränkungen können die Ziele der Umfrage regelmäßig erreicht werden.

### 3 Datenschutz im Verwaltungsbereich des SWR

#### 3.1 *Der Splitter im Auge der Zuschauer und der Balken im eigenen Auge - die offenen Wunde Vertraulichkeitserklärung*

Mitarbeiterinnen und Mitarbeiter müssen auch nach der DSGVO **auf die Vertraulichkeit verpflichtet** werden. Dies ergibt sich aus einem Zusammenspiel der Artikel 4 Abs. 1, 29 und § 32 Abs. 4 DSGVO. Für den journalistischen Bereich wird dies zudem ausdrücklich in § 9 c Rundfunkstaatsvertrag (RStV) geregelt. Ich hatte deshalb schon Mitte Dezember 2017 einen **umfassenden Entwurf nebst Merkblatt** gefertigt und angeregt, auf dieser Grundlage die Unterschriften der Mitarbeiter einzuholen. Nach zahlreichen Diskussionen und Intranet-Veröffentlichungen hat die Hauptabteilung Personal und Rechtemanagement am 7. Mai 2018 die Verpflichtung auf die Vertraulichkeit nebst Merkblatt versandt. Die Mitarbeiterinnen und Mitarbeiter wurden gebeten, die Erklärung bis zum 25. Mai 2018 (Inkrafttreten der DSGVO) zu unterschreiben.

Ich habe schon im letzten Tätigkeitsbericht darauf hingewiesen, dass es eine erhebliche Anzahl von Mitarbeitern gab und **nach wie vor** gibt, die diese **Verpflichtung auf die Vertraulichkeit nicht unterschreiben** möchten. Es ist den Verantwortlichen im SWR auch **nach über eineinhalb Jahren nicht** gelungen diese Verpflichtung von allen Mitarbeiterinnen und Mitarbeitern einzuholen. Es gibt immer noch Personen, die sich **weigern oder einfach keine Erklärung** abgeben. Auch am 19. Dezember 2019 und damit 19 Monate nach Geltung der DSGVO gibt es **immer noch 173 Mitarbeiter**, die trotz einer Erinnerungsmail keine Erklärung abgegeben haben. Es ist schon erstaunlich, dass sich darunter auch Journalisten befinden, die gerne den **Splitter im Auge von Unternehmen oder Behörden** sehen, aber wohl **nicht gewillt** sind, sich **selbst** zu verpflichten, ordnungsgemäß mit überlassenen Computern umzugehen und sich **datenschutzkonform zu verhalten**. Der verantwortliche Personalbereich im SWR will jetzt zwar nochmals diese 173 Mitarbeiter erneut anschreiben, danach aber lediglich einen Vermerk über die Weigerung in die Personalakte aufnehmen, jedoch anscheinend **keine arbeitsrechtlichen Maßnahmen** ergreifen.

#### 3.2 *Vertrauliche Leiharbeit?*

Bereits in meinem letzten Tätigkeitsbericht hatte ich ausführlich über die Einführung der Verpflichtung auf die Vertraulichkeit beim SWR berichtet. Im Nachgang hat mich die

Anfrage erreicht, ob auch Leiharbeitnehmer auf die Vertraulichkeit zu verpflichten sind. Dabei war unklar, ob der SWR diese Mitarbeiter selbst verpflichten darf oder ob dies Aufgabe des Verleihers ist, der seine Mitarbeiter an den SWR entleiht. Im letzten Fall wäre die Verpflichtung der Mitarbeiter ausschließlich mittelbar über eine vertragliche Regelung möglich. Dankenswerterweise hat der Gesetzgeber jetzt für diesen Fall eine Lösung parat. Nach § 26 Abs. 8 Nr. 1 BDSG fallen auch Leiharbeitnehmer im Verhältnis zum Entleiher unter den **Beschäftigtenbegriff**. Das bedeutet, dass der Bundesgesetzgeber auch **Leiharbeitnehmer** des Entleihers **als Beschäftigte** einstuft und dem Entleiher so die Möglichkeit gibt, Mitarbeiter unabhängig von ihrer rechtlichen Beziehung auf die Vertraulichkeit verpflichten zu können. Es wäre auch nicht einzusehen gewesen, warum gerade für Leiharbeitnehmer Ausnahmen gelten sollten. Immerhin haben Leiharbeitnehmer in gleicher Weise Zugang zu den Systemen des SWR und damit auch zu personenbezogenen Daten. Dementsprechend habe ich die Verpflichtung auf die Vertraulichkeit in der Weise angepasst, dass sich die **Verpflichtung** in Anlehnung an den Gesetzestext **auch auf Leiharbeitnehmer** erstreckt.

### **3.3 Topfit im Datenschutz?**

Der SWR bot seinen Mitarbeitern mit der **Software Fit@work** eine Möglichkeit, sich sportlich am Arbeitsplatz zu betätigen. Fit@work ist nun etwas in die Jahre gekommen und benötigt zudem eine Installation auf dem Rechner. Daher sollte die Software durch eine moderne **webbasierte Anwendung** ersetzt werden. Die neue Software **Back2Action** bietet statt Fit@work aktuelle Übungsprogramme in einem frischen Design und eine Programmierung auf dem neuesten Stand der Technik. Darin haben die Mitarbeiter Zugang zu ein- bis dreiminütigen Videoclips mit Bewegungs-, Entspannungs- und Augenübungen am Arbeitsplatz.

Neben meiner datenschutzrechtlichen Prüfung umfangreicher Dokumente war zudem auch ein Auftragsverarbeitungsvertrag mit Back2Action zu schließen. Als problematisch stellte sich bei der Nutzung von Back2Action der Einsatz von **MailChimp** heraus. MailChimp wird für den Versand und auch für eine Analyse des Newsletters verwendet. Problematisch zum einen, da sich das Unternehmen in den USA befindet, und zum anderen, da sich mittels der Analyse feststellen lässt, ob eine Newsletter-Nachricht geöffnet und welche Links gegebenenfalls angeklickt wurden.

MailChimp kann zwar eine Zertifizierung nach dem **EU-US-Privacy-Shield** und damit derzeit ein angemessenes Datenschutzniveau bescheinigt werden. Jedoch ist zu erwarten, dass auch der Privacy-Shield (wie zuvor Safe-Harbor) auf Dauer keinen Bestand haben wird. Daher wäre es im Sinne einer **datenschutzfreundlichen Voreinstellung** wünschenswert gewesen, wenn der Nutzer die Bestellung des Newsletters bereits bei der Registrierung unterbinden hätte können. Allerdings wird der Newsletter auch eingesetzt, um zu prüfen, ob Back2Action überhaupt genutzt wird. Dies wirkt sich auf die Anzahl der benötigten Lizenzen aus und ist damit auch eine Kostenfrage für den SWR.

In Absprache mit dem Gesundheitsmanagement habe ich daher trotz meiner Bedenken grünes Licht für Back2Action gegeben. Immerhin lässt sich jeder Newsletter auch kurzerhand abbestellen.

### **3.4 Gympass**

Bei Gympass handelt es sich um einen Anbieter, der seinen Nutzern ein **Netzwerk an Sport-Einrichtungen** weltweit zur Verfügung stellt. Dabei tritt Gympass als Vermittler auf und bietet den Nutzern Verträge mit verschiedenen Preisstufen an, die sich in der Anzahl der zu nutzenden Sporteinrichtungen unterscheiden.

Für die Registrierung bei Gympass war zunächst ein sogenanntes **Token-Verfahren** angedacht. Dabei wird mittels Ausgabe von Zahlencodes eine Anmeldung ermöglicht, so dass keinerlei personenbezogene Daten angegeben werden müssen. Leider war seitens des Anbieters eine Registrierung über die dienstliche Mailadresse zwingend für die Legitimation, da das Angebot von Gympass nur Mitarbeitern des SWR zugänglich gemacht werden sollte. Um die dienstliche E-Mailadresse zu schützen, habe ich mangels technischer Möglichkeit vertraglich auf einen Wechsel hin zur Nutzung einer privaten Mailadresse hingewirkt. Eine **Weitergabe** persönlicher Informationen wie z.B. der Mailadresse an Dritte ist vertraglich explizit **ausgeschlossen**. Kurz nach Einführung von Gympass steht den Kollegen nun ein Test-Account zur Verfügung, um sich von Gympass ohne Registrierung ein Bild machen zu können. Somit lässt sich auch ohne Angabe von Daten nach Gympass-Partnern in einer Umkreissuche recherchieren.

### 3.5 *eAbrechnung endlich sicher*

Schon vor Jahren bestand die Überlegung, den Beschäftigten elektronische Zugriffe auf diejenigen Dokumente zu erlauben, die ihnen aufgrund von Gesetzen, Tarifverträgen oder Dienstvereinbarungen zugänglich zu machen sind (und nicht in gedruckter Form zur Verfügung zu stellen sind). Inzwischen sind dies die Bescheinigungen zur Sozialversicherung, zur Lohnsteuer für das Kalenderjahr, die Nachweise für die Gleitzeit, die Zeitwertkonten und die Reiseabrechnungen sowie die monatlichen Verdienstabrechnungen.

Vor Jahren wurde deshalb damals unter Mitwirkung des Rundfunkbeauftragten für den Datenschutz die **Dienstvereinbarung** über den Schutz personenbezogener Daten mit Wirkung zum 1. Juli 2017 geändert. Einer der datenschutzrechtlichen Kernpunkte war die Bestimmung, dass die **Benutzererkennung nebst Passwort nicht ausreichend** ist, sondern ein weiteres spezielles Passwort notwendig ist. Im Laufe der technischen Umsetzung wurde dann eine **Zwei-Faktor-Authentifizierung** angestrebt. Die **Umsetzung** dauerte aber **fast zwei Jahre**. Erst im Juli 2019 war die überwiegende Anzahl der Nutzer erfolgreich registriert und eingerichtet. Das Zwei-Faktor-Verfahren funktioniert dergestalt, dass die Mitarbeiter nach ihrem Einloggen über das eAbrechnungssystem per Telefon aufgefordert werden, einen von ihnen selbst im Voraus festgelegten PIN-Code einzugeben. Die telefonische Aufforderung kann dabei über das dienstliche Telefon am Arbeitsplatz, aber auch über ein Smartphone erfolgen. Abgesehen von einem leisen Murren über die vermeintliche Umständlichkeit und dem einmal gegebenen Hinweis, es müsse nicht die private Handynummer angegeben werden, verlief die Einführung reibungslos. Einziger Kritikpunkt meinerseits ist die **lange Dauer der Einführung** von fast zwei Jahren, was zukünftig jedoch unter der Geltung der DSGVO schneller gehen muss.

### 3.6 *Des Pudels Kern*

Anfang des Jahres erreichten mich Anfragen zur Datenschutzerklärung auf SWR3. Auf den ersten Blick schien es sich dabei um Besucher der Website zu handeln, die von ihrem Beschwerderecht Gebrauch machen wollten. Auf meine Bitte, dies zu konkretisieren, erhielt ich Ausführungen zu einem datenschutzkonformen Einsatz von Cookies und allgemeine Anforderungen an rechtswirksame Einwilligungserklärungen. Es stellte sich heraus, dass es sich lediglich um die versuchte Akquise von Anbietern handelt, die dem SWR eine Softwarelösung zur Verwaltung von Einwilligungserklärungen anbieten wollten.

### **3.7 Datenschutz bei der SWR Media Services GmbH**

#### **3.7.1 Die Mutter aller Türme**

Bekanntlich ist der Fernsehturm in Stuttgart-Degerloch das Urmodell für die Fernsehtürme aus aller Welt. Nicht wenige sind der Meinung, dass der Fernsehturm in Stuttgart auch der Schönste aller Fernsehtürme ist. Zumindest ist er eines: Das Wahrzeichen der Stadt Stuttgart und der Region. Betrieben wird der Fernsehturm von der SWR Media Services GmbH, einer hundertprozentigen Tochtergesellschaft des SWR.

Zum Muttertag veranstaltete die SWR Media Services GmbH ein Gewinnspiel, bei dem nicht nur Aufzugstickets für Mütter und deren Kinder, sondern auch freier Eintritt zu den Yoga Sessions in luftiger Höhe zu gewinnen waren. Die Verlosung der Freitickets fand über den Social-Media-Kanal Instagram statt. Für die Teilnahme an der Verlosung sollten die Teilnehmer am Muttertag ein Foto zusammen mit ihrer Mutter von der Aussichtsplattform des Fernsehturms machen. Dieses Foto war dann mittels eines bestimmten Hashtags auf den Instagram-Kanal des Fernsehturms zu verlinken. Die Teilnahmebedingungen sollten dann aber doch ganz altmodisch auf der Website des Fernsehturms veröffentlicht werden. Dafür hielt der Datenschutzbeauftragte der SWR Media Services GmbH Rücksprache mit mir als seiner Aufsichtsbehörde, ob darin die Angaben zum Datenschutz im Hinblick auf die neuen Regelungen der DSGVO ausreichend beachtet sind. Nach einer Erörterung der Informationspflichten des Verantwortlichen konnten die Teilnahmebedingungen für das Gewinnspiel ohne Weiteres zum Abschluss gebracht werden.

#### **3.7.2 Datensicherheit**

Von dem Angriff auf einen SWR-Rechner (siehe Ziff. 5.2) war auch ein Server der SWR-Media Services GmbH betroffen.

## 4 Datenschutz beim ARD ZDF Deutschlandradio Beitragsservice

### 4.1 Grundlagen zum Rundfunkbeitrag

Mit der Reform der Rundfunkfinanzierung zum 1.1.2013 erfolgte die Umstellung auf eine **neue Finanzierungsform**. Die an Rundfunk- und Fernsehempfangsgeräte gebundene frühere **Rundfunkgebühr** wurde **durch** den **Rundfunkbeitrag ersetzt**, der im Privatbereich pro Wohnung erhoben wird unabhängig von der Zahl der darin gemeldeten Bewohner und der dort befindlichen Empfangsgeräte. Im geschäftlichen und gewerblichen Bereich wird an die Betriebsstätten angeknüpft.

Verwaltet werden die Daten der Rundfunkbeitragszahler (wie seither die der Gebührenzahler) zentral in Köln durch den „**ARD ZDF Deutschlandradio Beitragsservice**“. Spezielle Sachverhalte werden von den dezentralen Beitragsabteilungen in den einzelnen Landesrundfunkanstalten betreut.

Für die Kontrolle dieses zentralen Beitragsservices ARD ZDF Deutschlandradio sind, wie bereits vorher bei der GEZ, die Datenschutzbeauftragten der einzelnen Rundfunkanstalten jeweils für ihren Teilnehmerkreis nach Maßgabe des für die Rundfunkanstalt geltenden Rechtes zuständig. Die Ausnahme bilden die Länder Berlin und Brandenburg (rbb), Bremen (rb) und Hessen (hr). Hier üben die Landesdatenschutzbeauftragten die Kontrollfunktion aus. Unter dem Gesichtspunkt der Staatsferne des Rundfunks ist dies verfassungsrechtlich höchst bedenklich. Denn die Landesdatenschutzbeauftragten wirken damit als staatliche Fremdkontrollorgane in die Rundfunkanstalten hinein und zwar insbesondere in dem für Rundfunkanstalten existenziellen und auch verfassungsrechtlich besonders sensiblen und geschützten Bereich der Rundfunkfinanzierung (Knothe/Potthast, Festschrift für Hans-Dieter Drewitz, Nomos-Verlag, S. 167 f.).

Für die Daten der fast 7,4 Mio. privaten **Rundfunkbeitragskonten** im **Sendebereich des SWR**, also Baden-Württemberg und Rheinland-Pfalz, gelten materiell die **Vorschriften des Rundfunkbeitrags-Staatsvertrages** und ergänzend das Landesdatenschutzgesetz Baden-Württemberg (aufgrund § 39 Abs. 1 SWR-Staatsvertrag; vgl. Anhang Ziff. 9.1). Für die **Kontrolle** ist ausschließlich der **Rundfunkbeauftragte für den Datenschutz** im SWR zuständig.

Routinemäßige Datenschutzaufgaben im Bereich des Gebühreneinzugs werden gemäß § 11 Abs. 2 RBStV von der internen Datenschutzbeauftragten des zentralen Beitragsservice vor Ort in Köln wahrgenommen. Sie ist oft erste Ansprechpartnerin bei Datenschutzbeschwerden ([datenschutz@beitragsservice.de](mailto:datenschutz@beitragsservice.de)). Als Mitglied des Arbeitskreises der Rundfunkdatenschutzbeauftragten ist sie zudem ins Netzwerk der Kontrolle im Rundfunkbereich eingebunden (vgl. Ziff. 7.6).

#### **4.2 Datenbestand beim zentralen Beitragsservice und beim SWR**

Der Beitragsservice in Köln ist eine nicht-rechtsfähige **Gemeinschaftseinrichtung** von ARD, ZDF und Deutschlandradio und für die Abwicklung des Beitragseinzugs und die Verwaltung der rund 44,5 Millionen Beitragskonten zuständig.

Der Anteil der **SWR-Beitragszahler** am Gesamtaufkommen liegt bei etwa 7,4 Mio. privaten und ca. 673.000 nicht-privaten (also geschäftlichen) Rundfunkbeitragskonten bei ca. 18,1 % des Gesamtbeitragsaufkommens. Damit ist der SWR nach wie vor die zweitgrößte Landesrundfunkanstalt innerhalb der ARD nach dem WDR und vor dem NDR als drittgrößtem Sender.

Wie bei allen Landesrundfunkanstalten verfügt auch der SWR über eine **eigene dezentrale Abteilung** für die Rundfunkbeitragsabwicklung. Die Zahl der Mitarbeiter ist in den letzten Jahren deutlich reduziert worden, weil mit der Umstellung auf den Rundfunkbeitrag einige Aufgaben entfallen oder vom zentralen Beitragsservice in Köln übernommen worden sind.

#### **4.3 Meldedatenabgleich**

Am 6. Mai 2018 startete der **Meldedatenabgleich** 2018 zum Rundfunkbeitrag. Der Beitragsservice von ARD, ZDF und Deutschlandradio gleicht ab diesem Tag die Daten aller volljährigen Bürgerinnen und Bürger der Einwohnermeldeämter mit seinen Bestandsdaten ab. Ziel des Meldedatenabgleichs ist es zu klären, für welche Wohnungen bislang kein Rundfunkbeitrag entrichtet wird. Wer keiner bereits zum Rundfunkbeitrag angemeldeten Wohnung zugeordnet werden kann, wird angeschrieben und um Rückmeldung gebeten, ob eine Anmeldung notwendig ist. Melden die angeschriebenen Personen zurück, dass für die Wohnung bereits ein Beitrag gezahlt



wird und teilen die entsprechende Beitragsnummer mit, werden ihre Daten unverzüglich gelöscht. Erfolgt eine Rückmeldung, dass noch kein Beitrag gezahlt wird, oder bleibt eine Reaktion aus, so wird eine Anmeldung vorgenommen. Im Hinblick auf **datenschutzrechtliche Beschwerden** lässt sich feststellen, dass man aufgrund der einen oder anderen Beschwerde den Eindruck gewinnen konnte, dass die Qualität der Meldedaten bei den Einwohnermeldeämtern nicht immer ganz optimal ist.

## 5 Datensicherheit im SWR

Im Jahre 2019 gab es mehr Hackerangriffe denn je. Auch der SWR war nicht verschont davon. Dies passt zum Sicherheitsbericht der Firma Akamai. Danach konzentrieren sich 35 % der Angriffe auf Webanwendungen der Medien- und Technologiebranche. Diese Angriffe geschehen insbesondere mit Hilfe gestohlener Anmeldedaten (Benutzername, E-Mail-Adresse) i.V.m. dem dazugehörigen Passwort. Derartige „Credential-Stuffing-Angriffe“ haben das Ziel, anfällige Server zu finden, um schädlichen Programmcode zu verbreiten oder Erpressungsprogramme („Ransomware“) einzusetzen. Fast 70 % der Angriffstypen beziehen sich auf eine sogenannte *SQL-Injection* und weitere über 20 % auf *Local File Inclusion*.

Attacken auf SWR-Rechner gibt es praktisch täglich und die meisten scheitern an der Firewall oder sonstigen Sicherheitsmaßnahmen. Angriffe können sowohl direkt auf die SWR-Rechner erfolgen als auch mittelbar auf die Computer von Dienstleistern. Vier Fälle werden nachfolgend exemplarisch dargestellt.

### 5.1 *Phishingversuche durch gefälschte E-Mails*

Geradezu klassisch sind die Versuche, mit gefälschten E-Mails, die einen gefährlichen Anhang haben oder bereits beim Öffnen Schadsoftware einschleusen, Schaden anzurichten oder den SWR auszuspionieren. Im Mai 2019 war auch der SWR von einer dieser üblichen Phishing-Attacken betroffen. Dabei wurden gefälschte E-Mails, nämlich solche, die angeblich von einem SWR-Mitarbeiter stammen, an eine Vielzahl von Mitarbeitern verschickt. Diese Mails waren versehen mit der Bitte, ein Dokument zu öffnen, was dann zur Folge gehabt hätte, dass sich Schadsoftware im SWR einnistet. Da dies frühzeitig erkannt worden war, konnten die Mitarbeiterinnen und Mitarbeiter über eine Warnmeldung vorab informiert werden.

### 5.2 *Angriff auf einen SWR-Server*

Im August 2019 wurde aufgrund eines Hinweises einer Sicherheitsfirma festgestellt, dass ein **SWR-Server** eine **Schwachstelle** hatte, was wohl zum Abzug von Daten geführt hat. Die Lücke wurde dann geschlossen, aber bei der folgenden Untersuchung wurde festgestellt, dass dort auch noch personenbezogene Daten gespeichert waren, die eigentlich schon längst hätten gelöscht werden müssen. Nachdem ich als Aufsichtsbehörde entsprechend Art. 33 DSGVO von der Datenpanne informiert worden

bin, habe ich geprüft, ob und inwieweit ein hohes Risiko entsprechend Art. 34 DSGVO besteht, mit der Folge, dass die betroffenen Personen zu benachrichtigen sind. Ich habe des Weiteren die Geschäftsleitung des SWR gebeten, die **Löschfristen und Löschungsrouinen zu überprüfen** und dafür Sorge zu tragen, dass nicht mehr benötigte Daten unverzüglich gelöscht werden. Erledigte Interaktionen mit Zuschauern, Gewinnspieldaten oder sonstige Kontaktdaten sind nach Ablauf der Aktion oder der Sendung nicht mehr erforderlich und es darf nur noch gemäß § 12 Abs. 1 SWR-Staatsvertrag und § 56 Abs. 2 Rundfunk-Staatsvertrag eine Aufbewahrung von drei Monaten bestehen.

### **5.3 Sicherheitsprobleme bei iPhones und iPads**

Im Juli 2019 wurde bekannt, dass auch iPhones und iPads dann angegriffen werden können, wenn keine aktuelle iOS-Version installiert ist. Daraufhin wurden vorsorglich alle Mitarbeiterinnen und Mitarbeiter gebeten, umgehend ein Software-Update für den Fall vorzunehmen, dass dies noch nicht geschehen ist.

### **5.4 Angriffe auf einen Dienstleister**

Mittelbare Angriffe und Gefährdungen der SWR-Rechner können sich über Cyber-Attacken bei Dienstleistern vollziehen, die mit dem SWR in Verbindung stehen. Im Mai 2019 wurde ein Dienstleister gehackt, der auf seinen Rechnern auch SWR Daten gespeichert hatte. Allerdings waren dies nur Daten über Standorte, Produktnamen sowie Modell- und Seriennummern bezogen auf den SWR. Nachdem der SWR vom Dienstleister informiert worden war, wurden beim SWR entsprechende vorsorgliche Schutzmaßnahmen ergriffen.

## 6. Auskunftersuchen und Beschwerden

Die Beschwerden über vermeintliche Datenschutzverstöße zogen zum Jahresende 2019 wieder stark an. Mit insgesamt **147 Beschwerden im Jahr 2019** wurden zwar die 179 im Jahr des Inkrafttretens der DSGVO 2018 nicht erreicht, doch die EU-Datenschutz-Grundverordnung sorgt wohl dauerhaft für erhöhte Beschwerdezahlen.

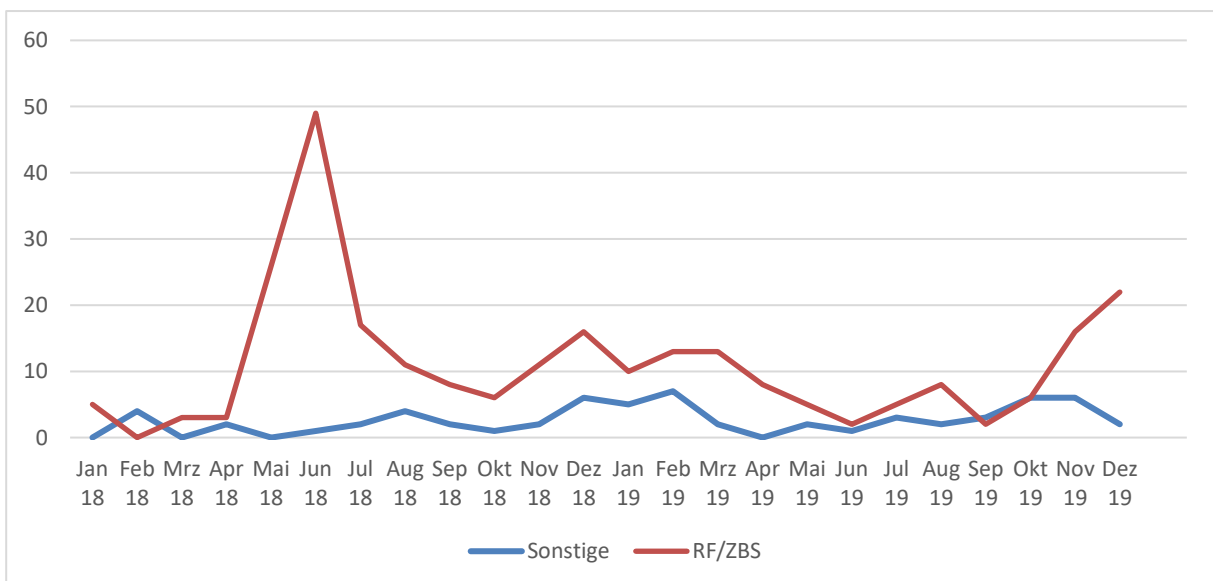
Zu verzeichnen waren

- sowohl für die **bei mir im SWR direkt** eingehenden **147 Vorgänge** (nachfolgend Ziff. 6.1),
- als auch die beim Zentralen **Beitragsservice** in Köln eingegangenen und den SWR betreffenden **1.361 Vorgänge** (nachfolgend Ziff. 6.2) zu.

### 6.1 Beim SWR eingegangene Auskunftersuchen und Beschwerden

Mit dem Inkrafttreten der DSGVO war es ab dem 25. Mai 2018 zu einem fulminanten Anstieg der Auskunftersuchen und Beschwerden gekommen und so waren es Ende 2018 schließlich 179 Auskunftersuchen und Beschwerden. Mit **147 Beschwerden im Jahr 2019** wurde diese Zahl zwar nicht erreicht, aber gegenüber der Zeit vor der DSGVO (mit unter 50 Beschwerden) ist dies immer noch eine gewaltige Erhöhung und Sorge macht der Anstieg zum Jahresende.

Die beiliegende Übersicht zeigt den Eingang im **Monatsverlauf der Jahre 2018 und 2019**:



### **6.1.1 Direkteingaben zum Rundfunkbeitragseinzug**

Von den insgesamt 147 Beschwerden, die bei mir im Jahr 2019 eingingen, betrafen **108** den **Rundfunkbeitragseinzug**.

Nach wie vor wird oftmals versucht, über das **Vehikel *Datenschutz*** zum beitragsrechtlich gewünschten Ergebnis (in der Regel: Keine Zahlungen leisten zu müssen) zu kommen. So wurde und wird die Löschung oder Berichtigung von Daten mit der Begründung verlangt, es liege kein Rundfunkbeitragsverhältnis vor. Daten seien zu Unrecht erhoben oder zu Unrecht von den Meldebehörden übermittelt worden. Auffällig ist, dass die meisten Eingaben mithilfe eines aus Internetforen heruntergeladenen Formbriefes bestehen. Es ist nicht immer einfach, den Beschwerdeführern klarzumachen, dass zuerst die beitragsrechtlichen Fragen zu klären sind.

Ich musste in fast allen Antwortschreiben **vorab** darauf hinweisen, dass es sich beim Rundfunkbeitragseinzug

- um strikten Gesetzesvollzug auf der Grundlage des als Landesgesetz erlassenen Rundfunkbeitrags-Staatsvertrages (RBStV) handelt,
- nach dem RBStV eine eindeutige und rigorose Zweckbindung besteht, weshalb auch keine kommerzielle Nutzung oder gar Verkauf der Daten erfolgt,
- weder Scorewerte gebildet, noch Persönlichkeitsprofile erstellt werden und keine Daten ins Ausland (nicht einmal innerhalb Europas) übermittelt werden.

Das Ziel, Auskunftsanfragen im Hinblick auf den Rundfunkbeitragseinzug innerhalb von 78 Stunden zu beantworten, konnte auch 2019 fast vollständig erreicht werden.

### **6.1.2 Sonstige Direkteingaben beim Rundfunkdatenschutzbeauftragten**

Wohl ausgelöst durch die Berichte über die EU-Datenschutz-Grundverordnung, wenden sich die Beschwerdeführer zunehmend den **Aktivitäten des SWR im Internet** zu, insbesondere der Präsenz auf Drittplattformen bzw. in den sozialen Medien sowie den Mediatheken. Dies wird kritisch und misstrauisch verfolgt. Für **Aktivitäten** in Bezug auf **Facebook**, sei es die Einbindung sogenannter „likes“ oder der **Aufbau von Fanpages**, haben die Beschwerdeführer regelmäßig kein Verständnis und kritisieren die Nutzung bzw. Zusammenarbeit mit einem Unternehmen, dessen Geschäftsmodell auf Datenschutzverstößen beruhe. Auch für mich ist der in den Programmen oft einseitige

Verweis auf Facebook statt auf die SWR-Websites im Internet (mit dem Argument, man müsse Zuschauer dort abholen, wo sie sich befinden) nicht überzeugend und datenschutzrechtlich fragwürdig. Allerdings ist die rechtliche Bewertung aufgrund der durch das Medienprivileg geschaffenen Ausnahmen schwierig. Ob der SWR – wie es ein Beschwerdeführer formuliert hat – letztlich nicht das Monster füttert, dass ihn fressen wird, kann nur die zukünftige Entwicklung der Medienlandschaft zeigen.

## **6.2 Anfragen und Auskunftersuchen beim Beitragsservice in Köln**

Gehen Fragen oder **Beschwerden** direkt **beim Zentralen Beitragsservice in Köln** ein, so antwortet grundsätzlich die betriebliche Datenschutzbeauftragte des Beitragsservice. Eingaben von Rundfunkteilnehmern aus dem Sendegebiet des SWR, die über einen Routineschriftwechsel hinausgehen oder datenschutzrechtliche Grundsatzfragen betreffen, beantworte ich ebenso selbst wie direkt beim SWR eingehende Anfragen oder Beschwerden (siehe oben Ziff. 6.1). Denn viele Betroffene wenden sich mit datenschutzrechtlichen Fragen beim Einzug der Rundfunkbeiträge auch direkt an mich.

Die Zahl der **Eingaben von Rundfunkteilnehmern** mit datenschutzrechtlichen Fragestellungen beim Beitragsservice ist im Jahr 2018 nach Inkrafttreten der EU-Datenschutz-Grundverordnung in die Höhe geschossen. Waren es 2016 insgesamt 831 Beschwerden und 2017 sogar nur 717, so waren es im Jahr 2018 *bis* zum Inkrafttreten der EU-DSGVO 497 und *danach* weitere 6.135, also zusammen 6.632. Jetzt im **Jahre 2019** hat sich die Zahl der „Datenschutzvorgänge“, die beim Beitragsservice in Köln eingingen, bundesweit **auf 10.417 erhöht**; dies entspricht einem **Anstieg von fast 60 %**. Von den 10.417 Eingaben aller Rundfunkteilnehmer betrafen 1.361 (also rund 13 %) das Sendegebiet des SWR.

## **6.3 Ausblick zu Auskunftersuchen und Beschwerden**

Beim Zentralen Beitragsservice in Köln war die Anzahl der Vorgänge zum Datenschutz im Dezember 2019 etwa doppelt so hoch wie jeweils in den davor liegenden Monaten. Beim SWR ist ein enorm starker Anstieg in den Monaten November und Dezember 2019 und auch bereits in den ersten Januarwochen 2020 festzustellen.

## 7 Organisation und Zusammenarbeit bei der Datenschutzkontrolle

### 7.1 Aufbau und Organisation auf europäischer Ebene

Wie die alte EG-Datenschutzrichtlinie 95/46/EG vom 24.10.1995, fordert auch die **EU-Datenschutz-Grundverordnung** die Errichtung von **Aufsichtsbehörden** (früher Kontrollstellen genannt). In den **Artikeln 51 ff. EU-DSGVO** werden hierzu konkrete Vorgaben gemacht. Die Aufsichtsorgane müssen **unabhängig** sowie **weisungsfrei** sein und keiner Dienst-, Fach- oder Rechtsaufsicht unterliegen.

Die Aufsichtsbehörden müssen nicht nur untereinander zusammenarbeiten, sondern auch mit dem neu geschaffenen **Europäischen Datenschutzausschuss** (Art. 68 EU-DSGVO). Im Gegensatz zu der Vorgängerorganisation (Art. 29 Gruppe) hat er weitreichende Aufgaben und Befugnisse. Eingebunden sind auch die EU-Kommission sowie der **Europäische Datenschutzbeauftragte** als Kontrollorgan für die Organe und Einrichtungen der EU (siehe oben Ziff. 1.2.1).

### 7.2 Aufbau und Organisation in Deutschland

Auch nach der **EU-Datenschutz-Grundverordnung** können in einem Land **mehrere Aufsichtsbehörden** errichtet werden. Deshalb gibt es **in Deutschland** folgende Aufsichtsorgane:

- der oder die Bundesdatenschutzbeauftragte,
- die Landesdatenschutzbeauftragten (in Bayern für den Bereich der Privatwirtschaft das Landesamt für Datenschutzaufsicht),
- die kirchlichen Datenschutzbeauftragten (siehe Art. 91 EU-DSGVO),
- die **Rundfunkdatenschutzbeauftragten** sowie
- die Datenschutzbeauftragten bei den Landesmedienanstalten.

Diese Vielfalt mag auf den ersten Blick verwirren, führt aber durch die mit den speziellen Materien vertrauten Aufsichten nicht nur zu einer höheren Kontrolldichte, sondern auch (ganz im Sinne des europäischen Subsidiaritätsprinzips) zu spezifischen und praxisgerechten Lösungen. Auch wenn Betroffene oft nicht die für sie zuständige Aufsichtsbehörde kennen, so ist dies in der Praxis regelmäßig unbedeutend, da eine

Verweisung an die zuständige Behörde bislang immer schnell und unproblematisch war und ist.

### **7.3 Aufbau und Organisation bei den Rundfunkdatenschutzbeauftragten**

Bereits vor Jahren hat der Europäische Gerichtshof festgestellt, dass der Mediendatenschutz vom nationalen und nicht vom europäischen Recht sicherzustellen ist (EuGH-Urteil vom 6.11.2003, Lindqvist ./ Schveden, C-101/01, RN 90). Für die **Rundfunkanstalten** besteht aufgrund Art. 5 GG sowie Art. 85 EU-DSGVO die verfassungsrechtliche Pflicht, eigenständige **Rundfunkdatenschutzbeauftragte** zu ernennen. Da der Bereich des Rundfunks zur **gesetzgeberischen Kernkompetenz der Bundesländer** gehört, obliegt die Ausgestaltung der Aufsichtsbehörden nach Art. 51 ff. EU-DSGVO den jeweiligen Bundesländern (unabhängig von der Frage der Gesetzgebungskompetenz der EU, vgl. oben Ziff. 1.4.1). Sie haben für „ihre“ Rundfunkanstalten die entsprechenden Regelungen zu treffen. Dies ist (nach dem Anstoß durch die EU-DSGVO) inzwischen für alle Rundfunkanstalten geschehen (näher oben Ziff. 1.4.1). Allerdings hat man das **verfassungsrechtliche Problem der gespaltenen Kontrolle** bei den drei Landesrundfunkanstalten (Radio Bremen, Hessischer Rundfunk und Rundfunk Berlin-Brandenburg) nicht gelöst, womit die staatlichen Landesdatenschutzbeauftragten für die Kontrolle des Verwaltungsbereichs zuständig bleiben, obwohl dieser untrennbar mit dem journalistischen Bereich verbunden ist.

### **7.4 Zusammenarbeit aller Aufsichtsbehörden auf nationaler Ebene**

Alle deutschen Datenschutz-Aufsichtsbehörden waren schon bislang sowohl nach deutschem Recht als auch nach Art. 28 Abs. 6 Satz 3 der alten EG-Datenschutzrichtlinie zur **Zusammenarbeit verpflichtet**, die Bundesdatenschutzbeauftragte hatte bereits nach dem alten BDSG (§ 26 Abs. 4) die ausdrückliche Aufgabe, koordinierend zu wirken.

Mit der **Geltung der EU-DSGVO** sind nicht nur deren **Regelungen zur Zusammenarbeit** zu beachten, sondern im neuen, ab 25. Mai 2018 geltenden BDSG vom 30. Juni 2017 (BGBl. 2017, S. 2097), wird in **§ 16 Abs. 5 BDSG** die Bundesdatenschutzbeauftragte verpflichtet, auf die Zusammenarbeit mit denjenigen Stellen hinzuwirken, die für den Datenschutz in den Ländern zuständig sind. Zudem **verpflichtet § 18 BDSG** die Aufsichtsbehörden des Bundes und der Länder **zur**



**Zusammenarbeit.** Aus Art. 51 Abs. 2 EU-DSGVO und dem Erwägungsgrund 119 ergibt sich, dass **alle Aufsichtsbehörden gleichwertig** und damit **gleich zu behandeln** sind. Eine Klassifizierung z.B. nach Größe (z.B. des Bundeslandes) oder Kontrollbereichen (z.B. öffentlich-rechtlich) ist nicht zulässig. Auch die Aufsichtsbehörden nach Art. 85 EU-DSGVO (Medien) sowie Art. 91 EU-DSGVO (Kirchen) sind gleichwertige Aufsichten nach Art. 51 Abs. 2 EU-DSGVO.

Nach dem Wortlaut des neuen **§ 18 Abs. 1 Satz 4 BDSG** soll eine **Beteiligung** dann erfolgen, wenn diese spezifischen Aufsichtsbehörden „von der Angelegenheit **betroffen** sind“. Wie sich aus dem weiten Aufgabenbereich der Rundfunkdatenschutzbeauftragten (vergleiche nur die in den Tätigkeitsberichten behandelten Themen und ihre Zuständigkeit auch für privatwirtschaftliche Beteiligungsunternehmen) ergibt, sind **Rundfunkdatenschutzbeauftragte** praktisch von **allen datenschutzrechtsrelevanten Gesetzen betroffen** und müssen daher zu praktisch allen Themen informiert und in diese eingebunden werden. Eine Einschränkung auf bestimmte juristische Bereiche oder eine „Vorabkontrolle“ durch die Landesdatenschutzbeauftragten (bzw. den BfDI), wann eine „Betroffenheit“ vorliegt, ist nicht mit dem europäischen Recht zu vereinbaren. § 18 Abs. 1 Satz 4 BDSG ist insoweit europarechtskonform auszulegen.

Leider haben einige Landesdatenschutzbeauftragte nach wie vor **Berührungsängste**, mit den Datenschutzbeauftragten der Kirchen und der Rundfunkanstalten zusammenzuarbeiten und versuchen nach außen den Eindruck zu erwecken, die Datenschutzkonferenz (DSK) sei die wahre und alleinige Vertretung der Datenschutzaufsichtsorgane in Deutschland. Inzwischen gibt es mehr oder weniger regelmäßige Treffen zwischen dem jeweiligen Vorsitzenden der DSK, dem Bundesdatenschutzbeauftragten, den Vertretern der öffentlich-rechtlichen Rundfunkanstalten, der Kirchen und Vertretern aus den Medienanstalten (sowie dem Presserat). Allerdings kann man **nicht** wirklich von einer **Zusammenarbeit** sprechen, sondern vielmehr von einem Informationsaustausch.

Nicht einmal in die Unterarbeitsgruppen der DSK ist eine Aufnahme als vollwertiges Mitglied erfolgt. In die Informationsflüsse, insbesondere aus dem Europäischen Datenschutzausschuss (Artikel 68 EU-DSGVO), sind die öffentlich-rechtlichen

Rundfunkanstalten vom Bundesdatenschutzbeauftragten nach wie vor nicht eingebunden.

Sinnvoller wäre es, im Interesse der Betroffenen und zum Schutz ihrer Persönlichkeit, alle Aufsichtsorgane gleichberechtigt einzubeziehen und zu beteiligen. Deshalb müsste die Datenschutzkonferenz (die rechtlich gesehen ein nicht-rechtsfähiger Verein ist) ihre Satzung ändern und auch die Rundfunkbeauftragten für den Datenschutz mit einbeziehen.

### **7.5 Zusammenarbeit der Datenschutzbeauftragten auf Länderebene**

Mit den **Landesdatenschutzbeauftragten** von **Baden-Württemberg**, Herrn Dr. Stefan Brink, **sowie** von **Rheinland-Pfalz**, Herrn Prof. Dr. Dieter Kugelmann, war und ist die Zusammenarbeit stets kooperativ.

### **7.6 Konferenz und Arbeitskreis der Rundfunkdatenschutzbeauftragten**

**Alle Datenschutzbeauftragten** der **öffentlich-rechtlichen Rundfunkanstalten** (ARD, ZDF, Deutsche Welle und Deutschlandradio) sowie die betriebliche Datenschutzbeauftragte des Zentralen Beitragsservice koordinieren ihre Datenschutzaufgaben in dem seit 1979 bestehenden Arbeitskreis AK DSB. Er tagt zweimal jährlich, besonders aktuelle und dringende Themen werden in Telefonschaltungen bzw. in Sondersitzungen beraten. Auch der Datenschutzbeauftragte des Österreichischen Rundfunks (ORF) nimmt regelmäßig an den Sitzungen teil. Der Arbeitskreis bietet Gelegenheit, Erfahrungen auszutauschen und anstaltsübergreifende Projekte gemeinschaftlich und zielgerichtet datenschutzkonform abzuwickeln. Hier werden auch die Interessen und Meinungen im Sinne der Mitwirkung bei gesetzgeberischen Vorhaben im Medien- und Datenschutzbereich gebündelt. Ab 1.1.2019 liegt der Vorsitz bei Herrn Dr. Heiko Neuhoff (NDR) und Herr Stephan Schwarze (MDR) ist sein Stellvertreter.

Als Folge der Regelungen der Datenschutz-Grundverordnung war es unumgänglich, dass sich diejenigen Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, welche die Aufsichtsfunktion nach Art. 51 ff. DSGVO wahrnehmen, zusammenschließen. Dies ist in der **Rundfunkdatenschutzkonferenz (RDSK)** geschehen. Sie hat sich inzwischen auch eine eigene Geschäftsordnung gegeben. Die

---

Mitglieder ergeben sich aus der Liste im Anhang (vgl. Ziff. 9.4). Die **RDSK** ist das **maßgebliche Organ**, welche die Aufgaben nach Art. 57 DSGVO und die Befugnisse nach Art. 58 DSGVO koordiniert. Sie will für eine einheitliche Anwendung der **Aufsichtsbefugnisse** sorgen und arbeitet mit dem inzwischen mehr im operativen Geschäft verhafteten AKDSB zusammen.

Zur Vereinheitlichung datenschutzrechtlicher Fragestellungen sollen zukünftig Entschlüsse, datenschutzrechtliche Eckpunkte oder Positionspapiere erarbeitet werden. Dies betrifft z.B. den Einsatz cloud-basierter Office-Systeme, datenschutzrechtliche Anforderungen beim Projekt SAP Prozessharmonisierung oder die Empfehlungen zum Einsatz von Cookies in Onlineangeboten der Rundfunkanstalten.

Das **Positionspapier** der Rundfunkdatenschutzkonferenz (RDSK) zum **IP-Autostart bei** der Nutzung von **HbbTV** (Hybrid Broadcast Broadband TV) vom Dezember 2019 ist dem Bericht als **Anlage** beigefügt.

## 8 Der Rundfunkbeauftragte für den Datenschutz im SWR

### 8.1 Rechtsgrundlagen

Die Aufgaben, Befugnisse und Stellung des Rundfunkdatenschutzbeauftragten ergaben sich ab dem 25. Mai 2018 aufgrund § 39 Abs. 1 SWR-Staatsvertrag aus dem (neuen) **Landesdatenschutzgesetz Baden-Württemberg** (LDSG BW) vom 12. Juni 2018 (GBl. BW, S. 173 ff.) sowie der unmittelbar geltenden EU-Datenschutz-Grundverordnung (EU-DSGVO).

### 8.2 Stellung des Rundfunkdatenschutzbeauftragten

Die **Stellung** des Rundfunkdatenschutzbeauftragten wird von den Artikeln 51 ff. EU-DSGVO sowie insbesondere **§ 27 LDSG BW** bestimmt. Er ist in Ausübung des Amtes völlig **unabhängig und nur dem Gesetz unterworfen**. Er unterliegt keiner Dienst-, Rechts- und Fachaufsicht. Die Finanzkontrolle des Verwaltungsrates darf seine Unabhängigkeit nicht beeinträchtigen.

Der SWR Verwaltungsrat ist auch dafür zuständig, dass der Rundfunkbeauftragte für den Datenschutz im SWR „angemessen“ vergütet wird (so § 27 Abs. 3 Satz 2 LDSG BW). Während beim Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten aufgrund der EU-Datenschutz-Grundverordnung nicht nur die Zahl der Planstellen erhöht wurde, sondern auch deren Vergütung, bewirkte die **DSGVO** beim SWR **keine Änderungen** (insbesondere auch nicht im Hinblick auf die **Vergütung**).

Der Rundfunkdatenschutzbeauftragte ist die anstelle des Landesbeauftragten für den Datenschutz zuständige **Aufsichtsbehörde nach Art. 51 EU-DSGVO** sowohl für den SWR als auch seine **Beteiligungsunternehmen** (insbesondere die **SWR-Media-Services GmbH**). **Innerhalb des SWR** ist es allerdings nicht immer ganz einfach, die **besondere Stellung** und Wertigkeit des Datenschutzbeauftragten als Aufsichtsbehörde zu verdeutlichen.

### 8.3 Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten

Die **Aufgaben und Befugnisse** eines Rundfunkdatenschutzbeauftragten ergeben sich über § 27 Abs. 7 LDSG BW aus den Artikeln 57 und 58 EU-Datenschutz-Grundverordnung (EU-DSGVO).

- Zu den **Aufgaben** gehört es nicht nur, die Anwendung der EU-DSGVO zu überwachen und durchzusetzen, sondern **Art. 57** enthält darüber hinaus einen Katalog mit 21 Pflichtaufgaben (z.B. von der Sensibilisierung der Verantwortlichen, betroffenen Personen und der Öffentlichkeit für Fragen des Datenschutzes bis hin zur Pflicht, mit anderen Aufsichtsbehörden zusammenzuarbeiten und Beiträge zur Tätigkeit des Datenschutzes des Europäischen Datenschutzausschusses zu leisten).
- In **Art. 58** sind die hoheitlichen **Befugnisse** einer Aufsichtsbehörde geregelt. Danach kann ein Verantwortlicher gegebenenfalls per Verwaltungsakt zu Handlungen oder Unterlassungen verpflichtet werden, insbesondere können Verarbeitungsvorgänge untersagt werden. Das Gesetz unterscheidet zwischen Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen und beratenden Befugnissen.

Gegenüber privatrechtlichen Unternehmen (z.B. der SWR-Media-Services GmbH) können sogar Bußgelder verhängt werden.

Gegenüber dem SWR selbst kann kein Ordnungswidrigkeitenverfahren eingeleitet werden, wohl aber gegenüber einzelnen Mitarbeiterinnen und Mitarbeitern, welche mit der Verletzung ihrer Dienstpflichten zugleich Datenschutzverstöße begehen.

#### **8.4 Regelungen zum Tätigkeitsbericht**

Der **Tätigkeitsbericht** des Rundfunkdatenschutzbeauftragten beim SWR war schon immer gegenüber den Organen des SWR zu erstatten und seit dem 1. März 2017 war er auch zu veröffentlichen (was dann auch unter [www.swr.de/datenschutz](http://www.swr.de/datenschutz) geschah und geschieht). Inzwischen hat der Gesetzgeber unter dem Eindruck von Art. 59 EU-DSGVO in § 27 Abs. 10 Satz 2 LDSG BW nicht nur den **Berichtsturnus** von zwei Jahren **auf ein Jahr abgesenkt**, sondern auch bestimmt: „Der Bericht wird den **Landtagen** und den **Landesregierungen** der unterzeichnenden Länder des Staatsvertrages über den Südwestrundfunk **übermittelt**.“

### **8.5 Tatkräftige Hilfe**

Bei der Erfüllung der Umsetzung des Datenschutzes im SWR unterstützen mich **Frau Elvira Scheppe und Herr Florian Schad**, denen ich an dieser Stelle **ausdrücklich danken** möchte.

Der Rundfunkbeauftragte für  
den Datenschutz beim SWR  
Prof. Dr. Armin Herb  
Neckarstraße 230  
70190 Stuttgart

Tel. +49 (0)711-929 13014  
Fax +49 (0)711-929 13019  
E-Mail: [datenschutz@swr.de](mailto:datenschutz@swr.de)  
[www.swr.de/datenschutz](http://www.swr.de/datenschutz)

## 9 Anhang

### Übersicht:

- 9.1 § 39 Staatsvertrag über den Südwestrundfunk gültig seit 01.01.2014
- 9.2 § 9c Rundfunkstaatsvertrag in der Fassung des 21. Rundfunkänderungs-Staatsvertrages; gültig seit 25.5.2018
- 9.3 § 27 Landesdatenschutzgesetz Baden-Württemberg (LDSG BW) vom 12.6.2018 (GBl. BW 2018, S. 173 ff.); gültig seit 21.6.2018
- 9.4 Liste der Datenschutzbeauftragten als Aufsichtsbehörden von ARD, ZDF, Deutsche Welle und Deutschlandradio im Jahre 2019

### 9.1 § 39 Staatsvertrag über den Südwestrundfunk

(GBl.BW 2013, S. 313 ff, GVBl. RP 2013, S. 557 ff.; zuletzt geändert zum 30. Juni 2015: GBl.BW 2015, S. 332 u. 747; GVBl.RP 2015, S. 108)

#### § 39 Datenschutz

(1) Für den Datenschutz beim SWR gelten vorbehaltlich des Satzes 2 die auf Rundfunkanstalten anwendbaren Bestimmungen des Datenschutzgesetzes des Landes in der jeweils gültigen Fassung, in dem der Dienort der Intendanz liegt. Der Rundfunkrat bestellt mit Zustimmung des Verwaltungsrats länderübergreifend eine Person zur oder zum Rundfunkbeauftragten für den Datenschutz, die die Einhaltung aller Bestimmungen über den Datenschutz beim SWR überwacht und in Ausübung ihres Amtes völlig unabhängig und nur dem Gesetz unterworfen ist.

### 9.2 § 9c Rundfunkstaatsvertrag in der Fassung des 21. Rundfunkänderungs-Staatsvertrages; gültig seit 25.05.2018

Der Rundfunkstaatsvertrag ist als Anhang zum Gesetz zum 21. Rundfunkänderungs-Staatsvertrag und zur Anpassung des Medien-Datenschutzrechts an die Verordnung (EU) 2016/679 vom 24. April 2018 (GBl. BW 2018, Seite 129 ff.) abgedruckt und in Kraft getreten am 25.5.2018. Die Änderung durch den 22. RfÄndStV (GBl.BW 2019, 27 ff.) ließ § 9c RStV unberührt.

#### Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag)

##### § 9c

##### Datenverarbeitung zu journalistischen Zwecken, Medienprivileg

(1) Soweit die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio oder private Rundfunkveranstalter personenbezogene Daten zu journalistischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis).

Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen Zwecken von der Verordnung (EU) 2017/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4. Mai 2016, S. 1; L 314 vom 22. November 2016, S. 72) außer den Kapiteln I, VIII, X und XI nur die Artikel 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Artikel 24 und Artikel 32 Anwendung. Artikel 82 und 83 der Verordnung (EU) 2016/679 gelten mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses gemäß den Sätzen 1 bis 3 sowie für unzureichende Maßnahmen nach Artikel 5 Abs. 1 Buchst. f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Die Sätze 1 bis 5 gelten entsprechend für die zu den in Satz 1 genannten Stellen gehörenden Hilfs- und Beteiligungsunternehmen. Die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio und andere Rundfunkveranstalter sowie ihre Verbände und Vereinigungen können sich Verhaltenskodizes geben, die in einem transparenten Verfahren erlassen und veröffentlicht werden. Den betroffenen Personen stehen nur die in den Absätzen 2 und 3 genannten Rechte zu.

(2) Führt die journalistische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen der betroffenen Personen oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, kann die betroffene Person Auskunft über die der Berichterstattung zugrunde liegenden, zu ihrer Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann oder
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Die betroffene Person kann die unverzügliche Berichtigung unrichtiger personenbezogener Daten im Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Die weitere Speicherung der personenbezogenen Daten ist rechtmäßig, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen erforderlich ist.

(4) Für die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio und private Rundfunkveranstalter sowie zu diesen gehörende Beteiligungs- und Hilfsunternehmen wird die Aufsicht über die Einhaltung der geltenden datenschutzrechtlichen Bestimmungen durch Landesrecht bestimmt. Regelungen des Rundfunkstaatsvertrags bleiben unberührt.



(5) Die Absätze 1 bis 4 gelten auch für Teleshoppingkanäle.

Soweit es um **Telemedien** geht, gilt der gleichlautende § 57 Rundfunkstaatsvertrag

**9.3 § 27 Landesdatenschutzgesetz Baden-Württemberg (LDSG BW)**  
vom 12.6.2018 (GBl. BW 2018, S. 173 ff.); gültig seit 21.6.2018. Die Änderung durch Art. 3 des Finanzausgleichsgesetzes vom 18. Dezember 2018 ließ § 27 unberührt und erhöhte lediglich in § 23 die Besoldung des Landesdatenschutzbeauftragten von B5 auf B6 (GBl.BW 2019, 1549, 1551).

### **§ 27 Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz**

(1) Der Südwestrundfunk ernennt für die Dauer von sechs Jahren eine Rundfunkbeauftragte für den Datenschutz oder einen Rundfunkbeauftragten für den Datenschutz, die oder der für alle Tätigkeiten des Südwestrundfunks und seiner Beteiligungsunternehmen nach § 16c Absatz 3 Satz 1 des Rundfunkstaatsvertrages an Stelle der oder des Landesbeauftragten für den Datenschutz zuständige Aufsichtsbehörde nach Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 ist. Die Ernennung erfolgt durch den Rundfunkrat mit Zustimmung des Verwaltungsrats. Die zweimalige Wiederernennung ist zulässig.

(2) Die oder der Rundfunkbeauftragte für den Datenschutz muss über die für die Erfüllung der Aufgaben und Ausübung der Befugnisse erforderliche Qualifikation, nachgewiesen durch ein abgeschlossenes Hochschulstudium, sowie über Erfahrung und Sachkunde, insbesondere im Bereich des Schutzes personenbezogener Daten, verfügen.

(3) Die Dienststelle der oder des Rundfunkbeauftragten für den Datenschutz wird bei der Geschäftsstelle des Rundfunk- und Verwaltungsrats eingerichtet. Die oder der Rundfunkbeauftragte für den Datenschutz ist angemessen zu vergüten. Nähere Bestimmungen, insbesondere die Grundsätze der Vergütung, trifft der Rundfunkrat mit Zustimmung des Verwaltungsrats in einer Satzung. Ihr oder ihm ist die für die Erfüllung ihrer oder seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen. Die hierfür vorgesehenen Mittel sind jährlich, öffentlich und gesondert im Haushaltsplan des Südwestrundfunks auszuweisen und der oder dem Rundfunkbeauftragten für den Datenschutz im Haushaltsvollzug zuzuweisen. Die oder der Rundfunkbeauftragte für den Datenschutz ist in der Wahl ihrer oder seiner Mitarbeiterinnen oder Mitarbeiter frei. Sie unterstehen allein ihrer oder seiner Leitung.

(4) Das Amt der oder des Rundfunkbeauftragten für den Datenschutz kann nicht neben anderen Aufgaben innerhalb des Südwestrundfunks und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt der oder des Rundfunkbeauftragten für den Datenschutz zu vereinbaren sein und dürfen ihre oder seine Unabhängigkeit nicht gefährden. Das Amt endet mit Ablauf der Amtszeit, mit

Rücktritt vom Amt oder mit Erreichen des gesetzlichen oder tarifvertraglich geregelten Renteneintrittsalters. Die oder der Rundfunkbeauftragte für den Datenschutz kann ihres oder seines Amtes nur enthoben werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Rundfunkrats auf Vorschlag des Verwaltungsrats; die oder der Rundfunkbeauftragte für den Datenschutz ist vor der Entscheidung zu hören.

(5) Die oder der Rundfunkbeauftragte für den Datenschutz ist in Ausübung ihres oder seines Amtes völlig unabhängig und nur dem Gesetz unterworfen. Sie oder er unterliegt keiner Dienst-, Rechts- und Fachaufsicht. Der Finanzkontrolle des Verwaltungsrats unterliegt sie oder er nur insoweit, als ihre oder seine Unabhängigkeit dadurch nicht beeinträchtigt wird. Die Mitglieder des Rundfunkrats und des Verwaltungsrats sind berechtigt, Anfragen an die Rundfunkbeauftragte für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz zu richten, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(6) Jeder kann sich an die Rundfunkbeauftragung für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch den Südwestrundfunk oder eines seiner Beteiligungsunternehmen nach Absatz 1 Satz 1 in seinen Rechten verletzt worden zu sein.

(7) Die oder der Rundfunkbeauftragte für den Datenschutz hat die Aufgaben und Befugnisse entsprechend Artikel 57 und Artikel 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679. Gegen den Südwestrundfunk dürfen keine Geldbußen verhängt werden. § 25 Absatz 4 gilt entsprechend mit der Maßgabe, dass die Mitteilung an die Intendantin oder den Intendanten unter gleichzeitiger Unterrichtung des Verwaltungsrats zu richten ist. Dem Verwaltungsrat ist auch die Stellungnahme der Intendantin oder des Intendanten zuzuleiten. Von einer Beanstandung und Unterrichtung kann abgesehen werden, wenn es sich um unerhebliche Mängel handelt oder wenn ihre unverzügliche Behebung sichergestellt ist.

(8) Die oder der Rundfunkbeauftragte für den Datenschutz hat auch für die Dauer von zwei Jahren nach der Beendigung ihrer oder seiner Amtszeit von allen mit den Aufgaben ihres oder seines früheren Amtes nicht zu vereinbarenden Handlungen und entgeltlichen oder unentgeltlichen Tätigkeiten abzusehen.

(9) Die oder der Rundfunkbeauftragte für den Datenschutz ist während und nach Beendigung ihres oder seines Amtsverhältnisses verpflichtet, über die ihr oder ihm amtlich bekannt gewordenen Angelegenheiten und vertraulichen Informationen Verschwiegenheit zu bewahren. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden ist, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, der Informantenschutz zu wahren.

(10) Die oder der Rundfunkbeauftragte für den Datenschutz erstattet den Organen des Südwestrundfunks jährlich einen Tätigkeitsbericht nach Artikel 59 der Verordnung (EU) 2016/679. Der Bericht wird den Landtagen und den Landesregierungen der unterzeichnenden Länder des Staatsvertrags über den Südwestrundfunk übermittelt. Der Bericht wird veröffentlicht.

#### 9.4 Liste der Aufsichtsbehörden nach Artikel 51 ff. DSGVO über ARD, ZDF, DW, DLR

Rundfunkanstalten	Datenschutzaufsicht	Anschrift
BR	Dr. Reinhart Binder kontakt@rundfunkdatenschutz.de	Marlene-Dietrich-Allee 20 14482 Potsdam
Deutsche Welle	Thomas Gardemann datenschutz@dw.de	Kurt-Schumacher-Straße 3 53113 Bonn
Deutschlandradio	Dr. Reinhart Binder kontakt@rundfunkdatenschutz.de	Marlene-Dietrich-Allee 20 14482 Potsdam
Hessischer Rundfunk	Ulrich Göhler datenschutz@hr.de	Bertramstraße 8 60320 Frankfurt
Mitteldeutscher Rundfunk	Stephan Schwarze rundfunkdatenschutz@mdr.de	Kantstraße 71-73 04275 Leipzig
Norddeutscher Rundfunk	Dr. Heiko Neuhoff datenschutz@ndr.de	Rothenbaumchaussee 132 20149 Hamburg
Radio Bremen	Anna-Katharina Puschmann datenschutz@radiobremen.de	Diepenau 10 28195 Bremen
Rundfunk Berlin Brandenburg	Anke Naujock-Simon datenschutz@rbb-online.de	Masurenallee 8-14 14057 Berlin
Saarländischer Rundfunk	Dr. Reinhart Binder kontakt@rundfunkdatenschutz.de	Marlene-Dietrich-Allee 20 14482 Potsdam
Südwestrundfunk	Prof. Dr. Armin Herb datenschutz@swr.de	Neckarstraße 230 70190 Stuttgart
WDR	Dr. Reinhart Binder kontakt@rundfunkdatenschutz.de	Marlene-Dietrich-Allee 20 14482 Potsdam
ZDF	Dr. Reinhart Binder kontakt@rundfunkdatenschutz.de	Marlene-Dietrich-Allee 20 14482 Potsdam

## 9.5 Positionspapier der Rundfunkdatenschutzkonferenz (RDSK):



### **Positionspapier der Rundfunkdatenschutzkonferenz (RDSK) zum IP-Autostart bei der Nutzung von HbbTV**

Bei HbbTV (Hybrid Broadcast Broadband TV) kann sowohl das Rundfunksignal (Broadcasting) als auch das Breitbandinternet (Broadband) genutzt werden, um den Fernsehzuschauerinnen und -zuschauern neben der Rundfunksendung weitere Zusatzinformationen anzubieten. Bei Nutzung des Breitbandinternets wird bereits bei Aufruf eines Senders mittels einer über das Rundfunksignal versandten URL automatisch eine Internet-Verbindung zum Server des HbbTV-Anbieters hergestellt. Dadurch werden die Zusatzinformationen schon vor dem Drücken des Red-Buttons auf der Fernbedienung im Hintergrund geladen. Dies ist bei Nutzung der Online-Verbindung vom HbbTV-Standard so zwingend vorgegeben und hat u.a. zur Folge, dass die Zusatzangebote den Zuschauerinnen und Zuschauern unmittelbar nach dem Drücken des Red-Button ohne zeitliche Verzögerung zur Verfügung stehen.

Die Rundfunkdatenschutzkonferenz (RDSK) vertritt dazu folgende Rechtspositionen:

1. Die Datenverarbeitung im Zusammenhang mit der Verbreitung von Rundfunkangeboten im HbbTV-Standard ist von der Öffnungsklausel in Art. 85 Abs. 2 EU-Datenschutzgrundverordnung (DSGVO) erfasst. Sie unterliegt daher der Kontrolle der rundfunkspezifischen Datenschutzaufsicht. Auch bei den Rundfunkanstalten mit einer gespaltenen Kontrollzuständigkeit (Radio Bremen, Hessischer Rundfunk, Rundfunk Berlin-Brandenburg und Deutsche Welle) sind die Angebote von einer staatlichen Aufsicht ausgenommen und unterliegen ausschließlich der Kontrolle der Datenschutzbeauftragten der Rundfunkanstalten.

2. HbbTV gehört zum gesetzlichen Auftrag der öffentlich-rechtlichen Rundfunkanstalten. Das folgt aus der verfassungsrechtlich verbrieften Bestands- und Entwicklungsgarantie des öffentlich-rechtlichen Rundfunks.
3. Der IP-Autostart ist auch nach Wirksamwerden der DSGVO rechtlich zulässig. Rechtsgrundlage für den IP-Autostart ist Art. 6 Abs. 1 lit. e) DSGVO in Verbindung mit den gesetzlichen bzw. staatsvertraglichen Aufgabenzuweisungen an die Rundfunkanstalten. Außerdem können sich die Rundfunkanstalten auch auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO („berechtigtes Interesse“) stützen.
4. Für die effiziente Nutzung der hybriden Zusatzangebote ist der IP-Autostart erforderlich. Nur auf diese Weise ist gewährleistet, dass die Nutzung der Zusatzangebote unmittelbar nach dem Drücken des Red-Button beginnen kann. Würde die IP-Verbindung erst nach dem Drücken des Red-Button aufgebaut, käme es zu einer unzumutbaren Verzögerung bei der Nutzung der Zusatzangebote. Zudem ist bei der DSMCC-Option die Speicherung einer Zustimmung der Nutzerin / des Nutzers nur bei einem kleinen Prozentsatz der Geräte möglich. Auch wäre eine Reihe von HbbTV-Zusatzangeboten (z.B. Internet Link Services bei DVB T2, Hinweisdienste etc.) nur noch mit signifikanten Umwegen für die Zuschauer zu realisieren. Außerdem käme es aufgrund der begrenzten Bandbreite zu nicht hinnehmbaren inhaltlichen Einschränkungen in der Darstellung und im Umfang des Angebots.
5. Ausweislich des „Digitalisierungsberichts 2019 Video“ verfügt inzwischen die Mehrheit der TV-Haushalte über ein internetfähiges TV. Das Angebot von hybriden Zusatzdiensten ist mittlerweile Standard. Der Anteil der on-demand genutzten TV-Inhalte (Mediatheken) steigt stetig. Mit diesen Entwicklungen hat sich auch das Bewusstsein der Zuschauerinnen und Zuschauer verändert. Ihnen ist bewusst, dass bereits mit der bei Installation ihres Gerätes hergestellten Verbindung zum Internet die Möglichkeit der Übertragung der IP-Adresse eröffnet ist. Wer sein Fernsehgerät mit dem Internet verbindet, der weiß, dass eine Kommunikation nur über eine IP-Adresse möglich ist. HbbTV ist heute der mit Abstand wichtigste und am meisten genutzte Weg zur Darstellung der öffentlich-rechtlichen Mediatheken auf TV-Geräten.
6. Die RDSK weist darauf hin, dass die IP-Adresse vor dem Drücken des Red-Button ausschließlich zur Übertragung von Zusatzangeboten und nicht zur Bildung von Nutzerprofilen genutzt werden darf.

*Stand: Dezember 2019*

## 10 Stichwortverzeichnis

AK DSB .....	41	IP-Autostart .....	42, 51, 52
Aufsichtsbehörden.....	38, 39, 40, 44, 49	Kommission zur Ermittlung des Finanzbedarfs (KEF) 13	
Auftragsverarbeitung.....	20	Landesdatenschutzgesetz .....	30, 43, 46, 48
Auskunftsersuchen .....	35, 37	Löschung.....	7, 17, 36
Beitragsservice.....	13, 30, 31, 35, 37, 41	Medienprivileg.....	37, 46
Berichtsturnus .....	44	Melddatenabgleich .....	31
Beschwerden .....	15, 32, 35, 36, 37	Melddatendatenabgleich.....	13
Bundesdatenschutzgesetz .....	10	RDSK.....	41, 42, 51, 52
Cookies .....	7, 8, 28, 42	Rundfunkbeitrag .....	30, 31
Datenminimierung.....	21, 24	Rundfunkstaatsvertrag .....	25, 46, 48
Datenschutzanpassungsgesetz .....	10	Scorewerte.....	36
Datenschutzaufsicht .....	38	SWR Media Services GmbH .....	29
Datenschutzbeschwerden .....	31	Telemediengesetz.....	8
Datenschutzerklärung.....	14, 17, 18, 22, 23, 28	TikTok.....	14, 15
Datenschutzfolgenabschätzung.....	7	Twitter .....	16, 23
Datensicherheit .....	29, 33	Umfragen .....	23, 24
Einwilligung.....	7, 10, 14, 17	Verpflichtung auf die Vertraulichkeit.....	19, 25
E-Privacy-Verordnung .....	8	Webcam.....	18
Europäischer Datenschutzausschuss .....	38	WhatsApp .....	15
Fanpages.....	36	Widerrufsrecht.....	17
gespaltene Kontrolle.....	39		