SOZIALE MEDIEN UP
DATENSCHUTZ DOWN

14. TÄTIGKEITSBERICHT
DES DATENSCHUTZBEAUFTRAGTEN

1. Januar – 31. Dezember 2021

Prof. Dr. Armin Herb

14. Tätigkeitsbericht

des Rundfunkbeauftragten für den Datenschutz des Südwestrundfunks

Prof. Dr. Armin Herb

Berichtszeitraum: 1.1.2021 bis 31.12.2021

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.; GBl.BW 2018, 1549, 1551) dem Rundfunkrat, dem Verwaltungsrat, dem Intendanten des SWR sowie den Landtagen und Landesregierungen Baden-Württemberg und Rheinland-Pfalz.

INHALTSVERZEICHNIS

Zusammenfassende Würdigung und Bilanz nach 33 Jahren

1 Zusammenfassende Würdigung

Die Pandemie und die **Umsetzung der EU-Datenschutzverordnung** (DSGVO) im SWR haben eines gemeinsam: Es dauert **länger als gedacht**. Der SWR hat das **Ziel** der Umsetzung **noch nicht erreicht** und man bekommt den Eindruck, dies wird dem Rundfunkbeauftragten für den Datenschutz überantwortet, anstatt eigenständige Anstrengungen zu unternehmen.

Der vorliegende Tätigkeitsbericht für das Jahr 2021 stellt wieder **im *ersten Abschnitt*** die unverminderten und immer **komplexer werdenden gesetzgeberischen Aktivitäten** dar. Herausragendes Ereignis war 2021 das neue „Telekommunikation-Telemedien-Datenschutz-Gesetz-TTDSG“. Die **Auslegung** der Datenschutzgesetze wird von seitenlangen Ausführungen des Europäischen Gerichtshofes (**EuGH**) **und** des **Europäischen Datenschutzausschusses** (EDSA) geprägt, der aber seine Auslegungshilfen („Guidelines“) im Stadium der öffentlichen Konsultation nur in Englisch verfasst.

Datenschutzfragen nehmen insbesondere **im Programmbereich** des SWR zu (***zweiter Abschnitt***). Die **Ausweitung** der SWR-Aktivitäten **im Onlinebereich** zum Teil mit (neuen) Mitarbeitern, für die Datenschutz ein Fremdwort ist, erhöhen den datenschutzrechtlichen Beratungsbedarf enorm. Die linearen Programme treten gegenüber neuen **Social-Media-Anwendungen** und **Apps** zurück. Die **Hinwendung zu Facebook, Instagram oder WhatsApp** ist ungebrochen. Immer neue Werkzeuge („Tools“) zur Reichweitenmessung („Tracking“) erfordern Auftragsdatenverarbeitungsverträge, die über das Datenschutzdezernat statt über die Fachabteilungen laufen. Es bedarf besonderer Anstrengungen, die Persönlichkeitsrechte der Zuhörer, Zuschauer und Internetnutzer, die immer kritischer werden, zu gewährleisten.

Einsparungen und Umstrukturierung lassen auch den Datenschutz **im Verwaltungsbereich** (***dritter Abschnitt***) nicht zur Ruhe kommen. Coronatests und Videokonferenzsysteme müssen datenschutzkonform sein.

Beim **Klassiker**, dem Datenschutz beim **Beitragsservice,** sind die DSGVO-Anforderungen unverändert hoch (***vierter Abschnitt***).

Keine Entspannung und eine ständige Gefahrenquelle sind – wie **im *fünften Abschnitt*** ausgeführt - die Angriffe auf die **Datensicherheit**.

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

Die Neustrukturierung und Organisation der Datenschutzkontrolle bei den öffentlich-rechtlichen Rundfunkanstalten bedeutet einen erhöhten Koordinationsaufwand und 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 die Darstellung des Rundfunkbeauftragten für den Datenschutz im SWR, dessen gesetzlich vorgegebene **Aufgabenerfüllung** durch die Überlast gefährdet ist, weshalb weitere Ressourcen nötig sind (***achter Abschnitt***).

2 Bilanz nach über drei Jahrzehnten

Dieser 14. Tätigkeitsbericht für 2021 ist mein letzter Bericht nach über 33 Jahren Amtszeit. Nach meiner Ernennung zum Datenschutzbeauftragten des damaligen **SDR (Süddeutscher Rundfunk)** zum 1. April 1988 (mit einer zweijährigen Berichtspflicht) schloss sich das Amt eines **Rundfunkbeauftragten für den Datenschutz beim SWR** an (mit jährlichem Bericht). Der Datenschutz in Wirtschaft und Verwaltung hat in diesen 33 Jahren Höhen und Tiefen erlebt. Dies galt besonders für die Implementierung des Datenschutzes im öffentlich-rechtlichen Rundfunk. Im Moment ist der Datenschutz zwar in der öffentlichen Meinung allgegenwärtig, aber beim SWR ist er wieder einmal auf einem Tiefpunkt: **Soziale Medien up** und **Datenschutz down**. Datenschutz wird inzwischen nur noch als Bürokratie und lästige Pflicht angesehen. Die vom Gesetzgeber für die öffentlich-rechtlichen Rundfunkanstalten geschaffene **doppelte Privilegierung**, sowohl im Hinblick

auf den Inhalt der datenschutzrechtlichen Regelungen als auch das Privileg eigener Aufsichtsorgane, wird nicht als Chance begriffen, sich umfassend um ein funktionierendes Datenschutzmanagement innerhalb des SWR zu kümmern. Der Datenschutzbeauftragte wird allein gelassen, hat nicht genügend Personal und es bleibt dem Zufall überlassen, welche Bereiche sich an ihn wenden oder auf welche Probleme er stößt. Die Umsetzung der Datenschutzvorschriften, vornehmlich der DSGVO, ist eine Aufgabe des Verantwortlichen und damit des SWR. Die Aufgabe des Rundfunkbeauftragten für den Datenschutz besteht vorwiegend in einer Kontrolle und der Beratung, nicht aber im operativen Geschäft. Der Verantwortliche ist verpflichtet, ein systematisches Datenschutzmanagement zu etablieren und nicht den Datenschutzbeauftragten nur mit Arbeit zu überhäufen.

Die neue Datenschutz-Grundverordnung hat den Aufsichtsorganen und damit dem Datenschutzbeauftragten scharfe Schwerter in Art. 58 DSGVO gegeben und es war wahrscheinlich mein Fehler, davon nicht Gebrauch zu machen, sondern auf die Überzeugung der Argumente gesetzt zu haben. Jetzt, da sich der SWR immer stärker als Fisch im Haifischbecken der sozialen Medien tummelt und die klassischen linearen Medien zurückgefahren werden, wird auch der Datenschutz mehr und mehr zurückgedrängt: **Soziale Medien up – Datenschutz down**.

Meine Tätigkeit und Amtszeit endet nach 33 Jahren und die **Zukunft der Institution** „Rundfunkdatenschutzbeauftragter für den Datenschutz beim SWR“ ist **mehr denn je offen**. Digitalisierung und Zeitgeist arbeiten gegen den Datenschutz als grundrechtlich verbürgten Persönlichkeitsschutz. Aber ohne eine Implementierung des Datenschutzes in der Organisation und den Geschäftsabläufen des SWR und ohne eine personell gestärkte Aufsicht, werden nicht nur die Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter, sondern auch die der Zuschauer, Zuhörer und Nutzer der SWR-Aktivitäten zunehmend verblassen.

Stuttgart im Januar 2022 Prof. Dr. Armin Herb

1 Entwicklung des Datenschutzrechts im Jahr 2021

Die **EU-Datenschutz-Grundverordnung** (DSGVO) vom 25. Mai 2018 ist in der Rechtswirklichkeit angekommen. Zahllose gerichtliche Entscheidungen sowohl beim Europäischen Gerichtshof (EuGH) als auch den nationalen Gerichten beschäftigen sich mit der Auslegung. Die Datenschutz-Aufsichtsbehörden in den Ländern produzieren am laufenden Band entsprechende Papiere zur Umsetzung. Doch insgesamt gesehen ist die **Umsetzung der DSGVO bis heute offen und umstritten**. Die Praxis in den Unternehmen und öffentlichen Stellen zeigt nach wie vor einen hohen Handlungsbedarf (was auch für den SWR zutrifft).

Nachfolgend wird die neue **Rechtsentwicklung** in Europa und Deutschland 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 inzwischen zwar in großem Umfang zahlreiche Papiere (fast durchweg nur in englischer Sprache), doch diese sind für die Praxis nur bedingt hilfreich, zumal sie auch oft von den Aufsichtsbehörden der Mitgliedstaaten unterschiedlich interpretiert werden.
- Der **Europäische Gerichtshof** (EuGH) nimmt jede Gelegenheit wahr, die Auslegung der DSGVO voranzutreiben. So hat sich der EuGH auch im Jahr 2021 mit einer Vielzahl von Auslegungsfragen beschäftigt.
- Die **Europäische Kommission** hat am 4. Juni 2021 zwei Durchführungsbeschlüsse zu den Standardvertragsklauseln für die Auftragsdatenverarbeitung und die außereuropäische Datenübermittlung, insbesondere bezogen auf Art. 28 sowie Art. 46 DSGVO, erlassen. Die beiden umfangreichen und in der Praxis schwer zu handhabenden gesetzlichen Vorgaben sind im Amtsblatt der Europäischen Union veröffentlicht worden (L 199 vom 7.6.2021, Seite 18 bis 30 sowie Seite 31 bis 61).

1.2 Weitere europäische Verordnungen und Richtlinien zum Datenschutz

1.2.1 ePrivacy-VO als Nachfolge der RiLi 2002/58 zur elektronischen Kommunikation

Das Trauerspiel um die sogenannte **ePrivacy-Verordnung** ging auch im Jahre 2021 weiter (vgl. Ziff. 1.2.1 des 13. TB). Die europäischen Rechtsanwender warten bis heute insbesondere auf Regelungen zu **Trackingverfahren und Cookies**.

1.2.2 Gesetzespaket für digitale Dienste („Digital Services Act Package")

Das von der **EU-Kommission** am 27. Mai 2020 vorgelegte Gesetzespaket für digitale Dienste befindet sich nach wie vor im Rechtsetzungsprozess. Dieses sog. „**Digital Services Act Package**" unterscheidet zwei Bereiche:

- Zum einen sollten **Regulierungsmaßnahmen für große Plattformen** mit erheblichen Netzwerkeffekten („Gatekeeper") geschaffen werden, um für mehr Fairness und Transparenz im Wettbewerb innerhalb des digitalen Binnenmarktes der EU zu sorgen.
- Zum anderen sollen zugleich **neue Vorschriften für digitale Dienste** geschaffen werden, die sich insbesondere mit den Pflichten von Hosting-Providern und Online-Plattformen sowie einer „Aufsicht über die Inhaltepolitik der Plattformen" befassen.

Diese Vorschläge für einen Digital Services Act (DSA) und einen Digital Markets Act (DMA) werfen auch Fragen zur **Kompetenzverteilung** zwischen der Europäischen Union und den Mitgliedstaaten **im Mediensektor** auf.

1.2.3 Europäische Regulierung der künstlichen Intelligenz

Künstliche Intelligenz (engl. *artificial intelligence*) soll und wird zunehmend in den unterschiedlichsten Lebensbereichen eingesetzt. Die EU-Kommission hat deshalb am 21. April 2021 einen Vorschlag für eine **Verordnung zur Regulierung der künstlichen Intelligenz** vorgelegt. Geplant ist eine risikobasierte Regulierung von KI-Systemen. Danach sollen KI-Systeme mit unannehmbarem Risiko verboten, Hochrisiko KI-Systeme (z. B. biometrische Identifizierung) mit gesetzlichen Vorgaben versehen werden und für KI-Systeme mit geringem Risiko gelten nur Transparenzpflichten.

1.3 Gesetzgebung im Bereich des Bundes

Der Bundesgesetzgeber hat auch im Jahr 2021 eine Vielzahl von Gesetzen mit Bezug zum Datenschutzrecht erlassen, welche oftmals in kürzester Zeit noch vor der Bundestagswahl im September 2021 durchgezogen wurden:

1.3.1 Unternehmensbasisdatenregistergesetz (UBRegG)

Das **Unternehmensbasisdatenregistergesetz** (UBRegG) vom 9. Juli 2021 (BGBl., Seite 2506) hat als Ziel, „die zentrale Speicherung aktueller und konsistenter Stammdaten zu Unternehmen“, was „über eine **bundeseinheitliche Wirtschaftsnummer für Unternehmen** als registerübergreifenden Identifikator“ erreicht wird (Bundesrats-Drs. 338/21, Seite 1). Dazu wird die Wirtschafts-Identifikationsnummer nach § 139 c der Abgabenordnung herangezogen. Das Gesetz gilt zwar nicht für den SWR, aber für seine Beteiligungsgesellschaft, die **SWR Media Services GmbH**.

Das UBRegG ist das Pendant zum sog. „**Registermodernisierungsgesetz**“ (RegMoG) vom 28. März 2021 (BGBl. S. 591). Hier wird **auf der Basis des steuerlichen Identifikationsmerkmales** eine Art Bürgernummer bzw. **Personenkennzeichen** eingeführt, welches lebenslang gilt, einmalig und unverwechselbar ist und bei praktisch allen behördlichen Maßnahmen herangezogen wird. Damit ist die **Steueridentifikationsnummer** ein **behördenübergreifendes Merkmal**, welches zukünftig an rund 50 Stellen zusätzlich gespeichert wird, etwa im Melderegister, im Führerscheinregister, bei der Renten-, Kranken-, Unfall- und Pflegeversicherung sowie im Rahmen der IHKs und der Handwerkerordnung. Mit diesem Gesetz kommt es quasi zu einer **vollständigen Registrierung und Katalogisierung der Persönlichkeit**. Auch die Rundfunkanstalten sind so genannte Registerbehörden. Jedoch bedarf die **Erhebung** des Merkmals für **Zwecke des Rundfunkbeitragseinzugs** einer speziellen Rechtsgrundlage und damit noch einer **Änderung des Rundfunkbeitragsstaatsvertrages** (RBStV).

1.3.2 Änderungen BetrVG und BPersVG: Betriebsrat und Personalrat keine datenschutzrechtlich Verantwortliche

Die Rechte und Pflichten der Datenschutz-Grundverordnung (DSGVO) treffen den „**Verantwortlichen**“ (Art. 4 Nr. 7 DSGVO). Bislang war strittig, ob neben dem Arbeitgeber

bzw. Dienstherrn auch der Betriebsrat bzw. Personalrat als eigenständiger Verantwortlicher gilt. Der **Gesetzgeber** hat jetzt eine **Klärung** vorgenommen:

- Im privatwirtschaftlichen Bereich ist ein Arbeitgeber jetzt im Hinblick auf den Betriebsrat „Verantwortlicher" (§ 79a BetrVG; BGBl. 2021, S. 1762).
- Im öffentlichen Bereich gilt für Behörden und öffentliche Stellen des Bundes, dass nunmehr ein Dienstherr auch im Hinblick auf die Tätigkeit des Personalrates als datenschutzrechtlich Verantwortlicher anzusehen ist (§ 69 BPersVG; BGBl. 2021, S. 1614, 1629).

Auch für den Bereich der Landesbehörden und öffentlichen Stellen der Länder wird man nun von einer entsprechenden Rechtslage bei den Personalvertretungen ausgehen müssen.

1.3.3 Änderungen beim betrieblichen Eingliederungsmanagement (SGB IX)

Die Regelungen in § 167 SGB IX **verpflichten alle Arbeitgeber** und damit auch den SWR, ein **betriebliches Eingliederungsmanagement** (BEM) anzubieten und durchzuführen, wenn ein Mitarbeiter innerhalb eines Jahres zusammen länger als 6 Wochen (zusammenhängend oder kumuliert) arbeitsunfähig war. Diese seit Jahren bestehende **Regelung** wurde jetzt durch Art. 7 des Gesetzes vom 2. Juni 2021 (BGBl. 2021, S. 1387, 1395) **erweitert**. Es wurde nämlich folgender Satz eingefügt: „Beschäftigte können zusätzlich eine Vertrauensperson eigener Wahl hinzuziehen." Diese **Vertrauensperson** kann der Ehe- oder Lebenspartner, ein Verwandter, Arzt (oder sonstiger Heilberuf, z. B. Physiotherapeut, Logopäde) sein, aber auch ein Rechtsanwalt, Rechtsbeistand oder ein Datenschutzbeauftragter. Für den Arbeitgeber und damit auch den SWR ist von Bedeutung, dass die Mitarbeiter in dem **BEM-Einladungsschreiben ausdrücklich** auf die Möglichkeit **hingewiesen** werden müssen, eine Vertrauensperson mitnehmen zu dürfen. Geschieht dies nicht, sind spätere krankheitsbedingte Kündigungen regelmäßig unwirksam. Auf meinen Hinweis will der SWR sein BEM-Einladungsschreiben der aktuellen Rechtslage anpassen.

1.3.4 Hinweisgeberschutzgesetz und EU-Richtlinie zum Whistleblowing

Ich habe bereits im letzten Tätigkeitsbericht darauf hingewiesen, dass die Europäische Union die Richtlinie 2019/1937 „zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“, erlassen und am 26. November 2019 im Amtsblatt veröffentlicht hat (ABl. L 305/17). Diese sogenannte **Whistleblower-Richtlinie** muss von den Mitgliedstaaten bis zum 17. Dezember 2021 in nationales Recht umgesetzt werden, was aber in Deutschland bislang nicht geschehen ist. Hier ist man nicht über Entwürfe für ein Hinweisgeberschutzgesetz hinausgekommen. Damit gilt für den SWR die Richtlinie ab 18. Dezember 2021 unmittelbar und verpflichtet ihn, ein entsprechendes Hinweisgebersystem zu etablieren. Obwohl ich nicht nur im letzten Bericht (Ziff. 1.2.2 des 13. TB 2020), sondern auch durch direkte Information auf die Notwendigkeit hingewiesen habe, wird erst im Laufe des Jahres 2022 langsam begonnen werden, ein solches System beim SWR aufzubauen.

1.3.5 IT-Sicherheitsgesetz 2.0 und Änderung BSI-Gesetz

Das **Bundesamt für die Sicherheit in der Informationstechnik** (BSI) ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Das BSI hat nicht nur Unterstützungsfunktionen, sondern kann auch den Betreibern sogenannter „kritischer Infrastrukturen“ Vorgaben und Auflagen machen. Zu den **kritischen Infrastrukturen** gehören diejenigen Firmen und Institutionen, die für Staat und Gesellschaft von wesentlicher Bedeutung sind. Durch eine Gesetzesänderung vom 23. Juli 2021 (BGBl. Seite 1982) zählen dazu auch „Unternehmen im besonderen öffentlichen Interesse“. Diese sind nicht nur zur Auskunft oder Meldung von Störfällen verpflichtet, sondern müssen auch Anordnungen bis hin zu Überwachungsmaßnahmen dulden.

1.3.6 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Mit den Gesetzen vom 23. Juni 2021 zur Modernisierung der Telekommunikation (BGBl. S. 1858) und dem TTDSG – Telekommunikation-Telemedien-Datenschutz-Gesetz (BGBl., S. 1982) wurden die datenschutzrechtlichen Vorschriften im Bereich der **Telekommunikation** und der **Telemedien neu geordnet**:

- Die Datenschutzvorschriften aus dem bisherigen Telekommunikationsgesetz (TKG), z. B. die Regelungen zum **Fernmeldegeheimnis**, wurden in den 2. Teil des TDDSG übernommen (§§ 13-18 TTDSG).

- Die Datenschutzvorschriften für Telemedien wurden (modifiziert) aus dem Telemediengesetz (TMG) in das TTDSG überführt (§§ 19-25 TTDSG). Dabei wurde in Anlehnung an die geltende ePrivacy-Richtlinie auch eine Norm für den Schutz der **Privatsphäre in den Endeinrichtungen** geschaffen (§ 25 TTDSG).

Die Normen gelten seit dem 1. Dezember 2021. Für deren Anwendung ist zunächst festzuhalten, dass die Vorschriften für personenbezogene Daten nur ergänzend zur DSGVO gelten.

Ferner muss eine Einordnung vorgenommen werden, was Telekommunikation und was Telemedien sind:

- Nach § 3 Nr. 59 TKG ist **Telekommunikation** „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“. Dabei ist die Bereitstellung von (technischen) Netzen unabhängig von der Frage, von welchen Diensten (z. B. Telefon oder Internetdienste wie E-Mail oder Webseiten) genutzt werden, vom Begriff der Telekommunikation umfasst.
- **Telemedien** sind nach § 1 Abs. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste oder Rundfunk sind. Telemedien sind damit praktisch alle Dienste, die über die (technischen) Kommunikationsnetze laufen. Vom Begriff der Telemedien und damit den Regelungen in den §§ 19-25 TTDSG wird also praktisch jeder erfasst, der eine eigene **Webseite** unterhält, E-Mails oder **Newsletter** versendet oder einen **Blog** betreibt. Nach der Gesetzesbegründung (Bundestagsdrucksache 19/27441, Seite 38) entspricht der Telemedienbegriff „dem europarechtlichen Begriff der Dienste der Informationsgesellschaft“ (vgl. auch Art. 4 Nr. 25 DSGVO).

Von großer Bedeutung in der Praxis ist die Regelung in § 25 TTDSG, welche den **Schutz der Privatsphäre in „Endeinrichtungen“** bezweckt. Eine Endeinrichtung ist nach § 2 Nr. 6 TTDSG jede „Einrichtung zum Aussenden, Verarbeiten und Empfangen von Nachrichten“, sofern sie an ein öffentliches Telekommunikationsnetz angebunden ist. Somit ist jedes Smartphone und Festnetztelefon ebenso eine Endeinrichtung wie jeder

Laptop, jedes Tablet oder jeder PC, der direkt mit dem Internet verbunden ist. Aber auch Geräte für die Smart Home-Anwendungen (die Gesetzesbegründung nennt Küchengeräte, Heizkörperthermostate, Alarmsysteme und Mähroboter) bzw. entsprechende Geräte in Kraftfahrzeugen fallen darunter.

Nach § 25 **Abs. 1** TTDSG ist die Speicherung von Informationen (z. B. in Form von **Cookies** bzw. das Tracking, also das Nachverfolgen des Nutzerverhaltens) auf einer Endeinrichtung nur mit **Einwilligung** (entsprechend Art. 7 DSGVO) zulässig. Nach § 25 **Abs. 2** TTDSG gibt es jedoch auch **Ausnahmen**, bei denen für die Speicherung keine Einwilligung notwendig ist. Dies betrifft beispielsweise die Speicherung solcher Informationen, die technisch unbedingt erforderlich sind oder wenn die Speicherung erforderlich ist, damit dem Nutzer der gewünschte Telemediendienst (wohl im Sinne einer einzelnen Funktion) zur Verfügung gestellt werden kann. Zulässig ist es deshalb, beispielsweise die bevorzugte Sprache für die Kommunikation zu speichern, nicht aber Marketing-Cookies oder solche zur personalisierten Reichweitenmessung.

1.4 Gesetzgebung im Bereich der Zuständigkeit der Länder

Auch im Kompetenzbereich der **Länder** werden **ständig neue Regelungen** mit Bezug zum Datenschutz erlassen. Im **Bereich des Rundfunkwesens** handeln die Länder dadurch, dass sie **Staatsverträge** abschließen, die dann von den Landesparlamenten in das jeweilige Landesrecht umgesetzt werden.

1.4.1 Medienstaatsvertrag (MStV) und Urteil zur Rundfunk-Beitragserhöhung

Seit 2020 gilt der **Medienstaatsvertrag (MStV)**, der eine umfassende Regulierung und eine „zeitgemäße Medienordnung“ beabsichtigt. Er wurde im Gesetzblatt der Länder veröffentlicht (z. B. GBl.BW 2020, S. 429 und GVBl.PR 2020, S. 377). Im Hinblick auf die Regelung des Datenschutzes erfolgte die Konkretisierung von Art. 85 DSGVO durch § 12 und § 23 MStV (vergleiche auch meinen Aufsatz in den Verwaltungsblättern für Baden-Württemberg, Dezember Heft 2020, Seite 492 ff.).

Durch den **Ersten Medienänderungsstaatsvertrag** sollte auch § 8 RFinStV (Rundfunkfinanzierungsstaatsvertrag) zum 1. Januar 2021 geändert werden. Die **Höhe des Rundfunkbeitrags** sollte von 17,50 Euro auf 18,36 Euro **angehoben** werden. Das Land Sachsen-Anhalt hat es aber unterlassen, den Änderungsstaatsvertrag zu ratifizieren, weshalb es zur Klage der öffentlich-rechtlichen Rundfunkanstalten vor dem **Bundesverfassungsgericht (BVerfG)** kam.

In seiner Entscheidung (Beschluss vom 20. Juli 2021; 1 BvR 2756/20) stellt das BVerfG Folgendes fest:
„Dieses Unterlassen verletzt die Rundfunkfreiheit der Beschwerdeführer aus Art. 5 Abs. 1 Satz 2 GG in der Ausprägung der funktionsgerechten Finanzierung des öffentlich-rechtlichen Rundfunks. Zur Gewährleistung der Rundfunkfreiheit in der dualen Rundfunkordnung gehört die Sicherung der Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks unter Einschluss seiner bedarfsgerechten Finanzierung (vgl. BVerfGE 119, 181 <214>m.w.N.; stRspr). Dementsprechend steht den öffentlich-rechtlichen Rundfunkanstalten ein grundrechtlicher Finanzierungsanspruch zu.“ (RN 74 und 75).

Die Folge des Urteils war eine **Erhöhung des Rundfunkbeitrages ab dem 1. August 2021** von 17,50 Euro auf 18,36 Euro.

Nachdem das Bundesverfassungsgericht seit Jahrzehnten seine schützende Hand über die öffentlich-rechtlichen Rundfunkanstalten hält und sich auch nicht durch europarechtliche Erwägungen beeinflussen lässt, war das Urteil letztlich keine Überraschung. Neu am Urteil war die folgende Feststellung: „*Die Erfüllung dieses Anspruchs obliegt der Ländergesamtheit als föderaler Verantwortungsgemeinschaft, wobei jedes Land Mitverantwortungsträger ist.“* (RN 75). Dies wurde im Rahmen der Kritik am Beschluss des BVerfG als Missachtung der demokratischen Willensbildung eines Landesparlaments gebrandmarkt.

2 Datenschutz im Programm- und Produktionsbereich des SWR

2.1 Corona Tests beim SWR

Aus verschiedenen Bereichen hat mich die Frage erreicht, was der SWR bei **Corona Tests** im Datenschutz zu beachten hat. Denn die Tests machen einen Umgang mit personenbezogenen Daten notwendig. Konkret ging es bei den Anfragen um das **Orchester des SWR** und um szenische Produktionen wie den Tatort und die Fallers. Denn neben den weiterhin bestehenden Hygienemaßnahmen setzt der SWR auf **verpflichtende Tests vor der Aufnahme von Dreharbeiten**, so dass nur „negativ" getestete Personen am Set mitwirken dürfen. Im Regelfall setzt der SWR auf Antigen-Schnelltests. PCR-Tests kommen aber insbesondere im Bereich der Produktion zur Anwendung. Für die **Tests** war zu berücksichtigen, dass die Daten der Getesteten **von einem Dienstleister verarbeitet** werden, wenn die Abstriche im Labor ausgewertet und im Falle eines positiven Ergebnisses für die Zuordnung dieser Personen an die Gesundheitsämter übermittelt werden. Zudem handelt es sich bei den Ergebnissen der Tests um Gesundheitsdaten und damit um sensible personenbezogene Daten.

Zunächst einmal war aber zu klären, ob die persönlichen Daten in das Online-System des Dienstleistungsunternehmens durch die Mitarbeiter selbst eingegeben oder zentral in einer Exceltabelle erfasst werden sollen. Während es für die Produktionen praktischer war, die Dateneingabe von den Mitarbeitern vornehmen zu lassen, da ansonsten z.B. Daten von Komparsen, die über Agenturen vermittelt werden, zusätzlich abgefragt werden müssten, präferierte die Orchesterleitung angesichts des Zeitmangels vor Konzerten eine zentrale tabellarische Datenerfassung. Bei beiden möglichen Varianten, die Daten zu erfassen und zu übermitteln, stellte ich bei meiner Prüfung fest, dass **mehr Daten abgefragt** werden sollten, als zunächst für die Zuordnung der zu testeten Personen notwendig waren. Der vollständige Datensatz war erst im Falle eines positiven Corona-Ergebnisses für die Übermittlung an die Gesundheitsämter erforderlich. Damit widersprach das vorgesehene Verfahren dem in Artikel 5 Abs. 1 Ziff. c DSGVO niedergelegten Grundsatzes der Datenminimierung, da die personenbezogenen Daten nicht auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt war. Aus

diesem Grund wurde das Registrierungsverfahren für das Online-System von Seiten des SWR entsprechend angepasst. Die Mitarbeiter konnten nun über den Registrierungs-Link entweder freiwillig den kompletten Datensatz in das System eingeben oder lediglich Name, Vorname und Geburtsdatum für die Zuordnung des Testergebnisses. In dieser abgespeckten Variante war der Datensatz um die Adresse des SWR, sowie die Telefonnummer und Mailadresse der Produktionsleitung zu ergänzen. Die Benachrichtigung über das Testergebnis erfolgte in diesem Fall durch die Produktionsleitung. Der Fall zeigt, dass sich Gesundheitsschutz und Datenschutz miteinander vereinbaren lassen.

2.2 Überarbeitete Datenschutzerklärung des SWR

Zu Beginn des Jahres 2021 kam es zu einer Neuausrichtung und **Überarbeitung der Datenschutzerklärung** des SWR. Hintergrund war, dass der Umfang der Erklärung seit Geltung der DSGVO und die stetig wachsende Einbindung von Angeboten in den sozialen Medien erheblich zugenommen hatten. Die bisherige Darstellung der Datenschutzerklärung auf mehreren Seiten bedurfte daher der Optimierung. So wurden die jeweiligen Textabsätze zu unterschiedlichen Themen nunmehr in zusammenklappbaren Akkordeon-Boxen untergebracht. Damit ließ sich die Datenschutzerklärung übersichtlich auf einer Seite darstellen, wodurch sich auch die Transparenz erhöhte.

Besonders hervorzuheben ist auch die nunmehr vorhandene Möglichkeit für den Besucher der SWR-Webseiten, **Einstellungen zum Datenschutz** an einer Stelle **zentral vornehmen** zu können. Dadurch entfällt nicht nur ein Overlay (Overlay bezeichnet eine Überlagerung von mehreren Programmteilen), das diese Funktionen bislang über der eigentlichen Seite liegend, dezentral bereitstellte. Vielmehr können die Besucher jetzt alle **Datenschutzeinstellungen direkt auf der SWR-Seite** vornehmen, ohne dass sie gezwungen sind, für einen Widerspruch oder das Abschalten von Funktionen auf die Webseiten von (Fremd-)Anbietern zu wechseln. Zudem kann der Besucher jetzt auch die **Anzeige von Inhalten über** die **sozialen Medien** generell erlauben, die zuvor nur als Zweiklick-Lösung verfügbar waren.

2.3 Keine Ortung und Bewegungsprofile von Mitarbeitern

Wenn **Reporter direkt** einen **Beitrag zum SWR-Fernsehen** oder zur Tageschau nach Hamburg als Live-Schalte senden wollen, benötigen sie eine entsprechende App für ihr Smartphone. Ein Beispiel für eine solche App ist die LiveU-Smart App. Diese App wird nicht irgendwo in der Welt gespeichert, sondern der SWR setzt auf die ARD On-Premise-Lösung. On-Premise bedeutet, dass die App auf den Rechnern oder **Servern des SWR** (ARD) und nicht in einer Cloud installiert wird. Eher zufällig fiel dem Fachbereich auf, dass es bei dieser Lösung in den standardmäßigen Voreinstellungen auch zu einem Zugriff auf den Standort des Verwenders kommen konnte. Damit war die **Ortung von Mitarbeitern** möglich und es ließen sich **Bewegungsprofile** erstellen. Dies widerspricht dem Grundsatz datenschutzfreundlicher Voreinstellungen nach Art. 25 DSGVO, wonach von Anfang an standardmäßig die sog. „Location Services“ ausgeschaltet sein müssen und es nur zu einer manuellen Aktivierung durch den Verwender kommen darf.

Erfreulicherweise hat der Fachbereich sofort reagiert, indem zunächst im Installations-Wikipedia im Intranet des SWR auf diesen Umstand an prominenter Stelle aufmerksam gemacht wurde. Zudem wurde ich umgehend über das Problem in Kenntnis gesetzt. Die Möglichkeit Positions-/Ortungsdaten anzuzeigen, musste in jedem Fall schnellstmöglich beseitigt werden, da eine derartige Funktion betrieblich nicht notwendig ist. Dementsprechend war die Funktion zu entfernen und zudem die bereits erhobenen Daten zu löschen. Dies hat der Fachbereich in Zusammenarbeit mit der Administration des ARD-Sternpunkts und dem Support des App-Anbieters unverzüglich umgesetzt und mit einem zusätzlichen Hinweis auf die Änderung der Einstellungen an die Verwender versehen.

2.4 Von der Schiefertafel zum Whiteboard

Will eine Gruppe von Mitarbeitern ein gemeinsames Ergebnis erarbeiten (oder ein Brainstorming durchführen) oder bestimmte Abläufe diskutieren und darstellen, so wurden früher dazu (Schiefer-)Tafeln oder Flipcharts bzw. Pinnwände verwendet. Heute kommen sogenannte **Whiteboards** zum Einsatz. Dies sind mit dem Computer verbundene interaktive digitale Großbildschirme. Das Angebot an Hard- und Software für diese Tafeln ist umfangreich und so ist es nicht verwunderlich, dass unterschiedliche Gruppen im SWR unterschiedliche Systeme testen bzw. einsetzen. Seit Mai 2021 gibt es einen Pilotbetrieb mit dem Produkt MURAL. Im Rahmen der Prüfung stellte sich heraus, dass bereits

zahlreiche andere Whiteboard-Anwendungen im SWR genutzt werden, vorbei an offiziellen Stellen. Das **datenschutzrechtliche Problem** bei MURAL besteht hier darin, dass die anfallenden Daten weder in Deutschland noch in der Europäischen Union verarbeitet werden, sondern in einem Drittland auf dem amerikanischen Kontinent (Domäne Kolumbien). Ein Hosting in der EU ist zwar avisiert, wird aber noch nicht durchgeführt und es existiert auch kein Zeitplan dazu. Ich habe deshalb frühzeitig klargestellt, dass eine **dauerhafte Ablage** in MURAL **ausgeschlossen** sein muss. Die Daten können zur Vorbereitung und Durchführung von entsprechenden Sitzungen zwar in MURAL festgehalten werden, die endgültigen Ergebnisse, Protokolle oder Zusammenfassung müssen aber nach Abschluss gelöscht und gegebenenfalls auf andere SWR Standard-Dateiablagen kopiert werden. Eine dauerhafte Datenablage in MURAL wäre unzulässig. Inzwischen erfolgten entsprechende Arbeitsanweisungen zur Umsetzung der datenschutzrechtlichen Anforderungen.

2.5 Über den Wolken, aber nicht in die Cloud

Ein Flug mit dem Zeppelin ist ein großartiges Erlebnis. Das dachte sich wohl auch die Redaktion von SWR 3 und veranstaltete das **Gewinnspiel "Zeppelinflug**". Zunächst wurde ein riesiger Zeppelin mit der Aufschrift „SWR 3" über das Sendegebiet geschickt. Die Hörerinnen und Hörer wurden aufgefordert, ein Bild dieses Zeppelins zu posten und an SWR 3 zu senden, um an dem Zeppelin-Gewinnspiel teilnehmen zu können. Leider war eine Teilnahme zunächst nur über die datenschutzkritischen Plattformen Facebook, Instagram und TikTok (dazu Ziff. 2.1 und 2.2 meines 12. Tätigkeitsberichts unter https://www.swr.de/unternehmen/organisation/taetigkeitsbericht-2019-100.pdf) möglich. Außerdem wurden die Teilnehmer aufgefordert, drei Freunde als Mitfahrer für den Flug zu benennen. Einer Beschwerde wegen habe ich schließlich von der Aktion erfahren und mich daraufhin an die Redaktionen gewandt und sie gebeten, die Hörer **nicht** ausschließlich auf **datenschutzkritische Plattformen** zu **locken**, sondern auch auf die SWR-Webseite zu verweisen. Schließlich habe ich die Redaktionen für die Problematik sensibilisiert, die sich aus der Aufforderung ergibt, drei Freunde als Mitfahrer zu benennen. Bevor ein Teilnehmer in Begleitung seiner Freunde am Gewinnspiel teilnehmen und später abheben kann, ist eine Verlinkung erforderlich, für die jedoch die **Einwilligung** der Freunde einzuholen ist.

2.6 Nutzungsmessung von Podcasts

Bereits in meinem letzten Tätigkeitsbericht habe ich über das Thema **Tracking**, also die Nachverfolgung von Aktivitäten eines Nutzers, berichtet (vgl. 2.3 in TB 13). Die Messung von Nutzungsdaten ist notwendig, damit der SWR seinen gesetzlichen Auftrag erfüllen kann. Denn ohne Kenntnis, ob das Programm bei den Rundfunkteilnehmern Anklang findet, lassen sich deren Rundfunkbeiträge nicht im Sinne des öffentlich-rechtlichen Programmauftrages verantwortungsvoll einsetzen.

Im Berichtszeitraum wurde ich darüber informiert, dass der SWR die **Nutzungsmessung von Podcasts** zukünftig nicht mehr selbst vornimmt, sondern **von einem Dienstleister** durchführen lässt. Dafür erhält die Firma Podigee Zugriff auf die Log-Dateien der Podcasts, die für Audio-On-Demand-Angebote bei einem Streaming-Dienstleister des SWR gespeichert sind. Unter Logdaten sind inhaltliche und zeitliche Angaben zur Nutzung, sowie IP-Adresse und Browserkennung zu verstehen. Die IP-Adressen der Nutzer werden für die Auswertung pseudonymisiert verarbeitet, da es gerade nicht darum geht, einzelne Nutzungssequenzen auszuweisen. Vielmehr werden die Ergebnisse der Auswertungen ausschließlich aggregiert, d. h. als zusammengefasste Datensätze verwendet, um sie auf einer graphischen Benutzeroberfläche, dem sogenannten Dashboard, anzuzeigen. Nach dem Verarbeiten der Daten aus den heruntergeladenen Log-Dateien werden diese temporären Dateien wieder gelöscht. Ein **Rückschluss auf einzelne Personen** ist dann **nicht mehr möglich**.

Doch auch wenn temporäre Daten für Auswertungen pseudonymisiert, aggregiert und letztlich wieder gelöscht werden, kommt es doch zu einer Verarbeitung personenbezogener Daten im Auftrag des SWR, für die die DSGVO den Abschluss eines Auftragsverarbeitungsvertrages (AV-Vertrag) vorsieht. Der mir zur Prüfung vorgelegte AV-Vertrag von Podigee erfüllte in einem Punkt zunächst nicht die gesetzlichen Anforderungen. Dies wurde aufgrund meines Hinweises schließlich mittels einer Ergänzungsvereinbarung ohne Weiteres korrigiert. Zuletzt wurde auch die Datenschutzerklärung des SWR um die Nutzungsmessung durch Podigee angepasst. Dies mit dem Hinweis auf eine Opt-Out-Möglichkeit für die Nutzer.

2.7 Nicht lernfähig? Schon wieder sensible Daten verbreitet

Mit sensiblen Daten ist besonders sorgsam umzugehen. Auf diese besondere Kategorie von Daten habe ich schon in meinem 13. TB unter 6.1.2 aufmerksam gemacht, als ich die mangelnde journalistische Sorgfalt im **Umgang mit sensiblen Daten** bei der Corona-**Berichterstattung auf Intensivstationen in Krankenhäusern** beklagt habe. Damals habe ich mich an die verantwortlichen Hauptabteilungsleiter gewandt und eindringlich darum gebeten, bei den Mitarbeiterinnen und Mitarbeiter ein Bewusstsein für diese Daten zu schaffen. Offensichtlich wurde mein Appell nicht oder nicht von allen gehört, denn im Berichtszeitraum haben mich erneut ähnlich gelagerte Beschwerden erreicht. Zum Schutz von sensiblen Daten ist es unbedingt erforderlich, sie bei der journalistischen Arbeit als solche zu erkennen und unkenntlich zu machen, was beispielsweise durch eine **Verpixelung** erreicht werden kann. Diese Datenschutz-Grundlagen sollte sich jede Journalistin und jeder Journalist aneignen und beherzigen.

2.8 Einsatz von Sprachassistenten

Der SWR bietet seine **Programminhalte** mittlerweile auch über die **Nutzung von Sprachassistenten** an, womit diese Geräte in den Abteilungen des SWR verstärkt zum Einsatz kommen. Problematisch ist dabei, dass es zu **unbeabsichtigten Aufzeichnungen** kommen kann. Wie sich dies z. B. bei Amazons Alexa über die Einstellungen verhindern lässt und auch automatisierte Löschungen von Aufzeichnungen möglich sind, hatte ich den Mitarbeitern des SWR in einem Intranet-Artikel erläutert. Nun gibt es aber eine ganze Reihe von Smart-Speakern und auch Aufzeichnungsmöglichkeiten in den verschiedensten Anwendungen, die über Smartphones, Tablets oder Laptops genutzt werden können. Daher hat der SWR beschlossen, interne Audioaufzeichnungen mit Hilfe von Sprachassistenten im SWR mit einer **Dienstanweisung an die Beschäftigten** zu regeln. Danach besteht grundsätzlich ein **Aufzeichnungsverbot** von Gesprächen mittels Sprachassistenten, um einen Eingriff in die Persönlichkeitsrechte der Beschäftigten zu verhindern. Eine Aufzeichnung ist somit nur noch **ausnahmsweise im Einzelfall** möglich, wenn eine **betriebliche Notwendigkeit** vorliegt und zudem die Anforderungen der Dienstanweisung für die Nutzung von Sprachassistenten eingehalten werden. Dabei gilt es für die Praxis aber noch einen ganz **wichtigen Punkt zu beachten**: Bei den Sprachassistenten reicht es nicht aus, wenn sie einfach ausgeschaltet sind. Ein

Mithören ist nur dann nicht mehr möglich, wenn das Gerät keinen Strom hat. Notwendig ist also immer, dass der **Strom abgestellt wird**. Daher empfehle ich, Smart-Speaker nur über Steckerleisten zu betreiben, die über einen Ein/Aus-Schalter verfügen. So wissen die Mitarbeiter, die in den Raum kommen, gleich, ob der Sprachassistent an und aktiv ist, wenn das rote Licht des Schalters leuchtet. Aus diesen Gründen wird auch in den Studios mit einem Rotlicht gearbeitet, um allen Beteiligten anzuzeigen, dass eine Sendung produziert und damit aufgezeichnet wird.

2.9 Sezierung der Nutzer über Reichweitenmessung und Tracking

Der SWR hat einen gesetzlichen Auftrag und finanziert sich aus Rundfunkbeiträgen. Deshalb muss jeweils genau prüft werden, ob ein Beitrag, sei er im Fernsehen, Hörfunk oder im Internet veröffentlicht worden, den gesetzlichen Anforderungen entspricht. Dies schließt die Prüfung ein, ob nicht Rundfunkbeiträge sinnvoller verwendet werden können als beispielsweise für einen Blog oder Newsletter mit nicht einmal einem Dutzend Nutzern. Die Medienforschung und die **Reichweitenmessung** haben eine lange Tradition, die beim Fernsehverhalten beispielsweise über die Messung der Einschaltquote erfolgt. So werden beispielsweise von der GfK (Gesellschaft für Konsumforschung) täglich Daten vom Vortag zum Nutzungsverhalten geliefert. Basis ist ein Panel aus 5.000 ausgewählten Haushalten (mit rund 10.500 Personen). Diese haben aber alle eingewilligt, womit eine datenschutzrechtliche Grundlage vorliegt.

Die **Nutzung des Internetverhaltens** ist demgegenüber weitaus schwieriger. Üblicherweise wird ein **Trackingverfahren** angewandt, also die Nachverfolgung des Nutzerverhaltens am Computer. **Google Analytics** ist ein solches Trackingtool von Google, das der Datenverkehrsanalyse von Webseiten (Webanalyse) dient. Dabei werden folgende Daten an die Server von Google gesandt:

- IP-Adresse des Gerätes,
- Adresse und HTML-Titel der besuchten Webseiten mit Datum und Uhrzeit sowie
- Daten zum Browser, Betriebssystem, zur Sprachauswahl und Bildschirmauflösung.

Google Analytics wird inzwischen von verschiedenen (auch anderen europäischen) Aufsichtsbehörden als äußerst datenschutzkritisch beurteilt.

Auch der SWR verwendet Trackingverfahren, auch wenn letztlich keine Personalisierung erfolgen soll, weil nicht der einzelne Nutzer, sondern die **Gesamtheit von Interesse** ist. Problematisch ist allerdings, dass man den Eindruck gewinnen kann, jede Redaktion und jeder Bereich nutze ein anderes Tool zur Messung des Nutzungsverhaltens (man braucht nur die SWR-Datenschutzerklärung lesen) und **datenschutzfreundliche Alternativen** (wie beispielsweise Matomo, ehemals Piwik, eine Open-Source-Webanalytik-Plattform, die von der schleswig-holsteinischen Datenschutzbehörde entwickelt wurde) mit dem Argument, sie seien nicht komfortabel, werden gar nicht in Erwägung gezogen.
Trackingverfahren gibt es auch im Rahmen des **Newsletter-Versandes**. So können in den HTML-Code von Newslettern **Trackingpixel** eingebaut werden, die dazu führen, dass beim Aufruf eines Newsletters der Versender informiert wird. Er erfährt dann, ob und wann welcher Nutzer den Newsletter geöffnet hat. Diese Informationen sind für den Versender eines Newsletters sicher interessant und können zur Optimierung führen, fraglich ist aber, ob dies datenschutzrechtlich ohne Einwilligung zulässig ist. Bezogen auf den SWR halte ich den Einsatz von Trackingpixeln ohne Einwilligung bzw. vertragliche Vereinbarung nur dann für zulässig, wenn die Erfassung der Informationen zwingend erforderlich ist, um den öffentlich-rechtlichen Auftrag einer Rundfunkanstalt zu erfüllen.

Kommt man zur Zulässigkeit des Setzens eines Trackingpixels ohne Einwilligung, so stellt sich nicht nur die Frage der Information der Bezieher der Newsletter, sondern auch, ob man Ihnen die Möglichkeit geben muss, das Trackingpixel „auszuschalten“, also zu deaktivieren.

3 Datenschutz im Verwaltungsbereich des SWR

3.1 Zeitwertkonten müssen gepflegt werden

Mitarbeiterinnen und Mitarbeiter des SWR werden durch einen entsprechenden **Tarifvertrag gezwungen**, monatlich bestimmte Beiträge abzuführen, die dann am Ende des Berufslebens in ein **Zeitguthaben** umgewandelt werden. Dadurch wird ein **früherer Ruhestand** erreicht. Über ein spezielles Portal kann man den aktuellen Stand einsehen. Bislang war es gängige Praxis, dass der Zugang zu diesem Zeitwertkonto automatisch gesperrt wurde, wenn man sich nicht innerhalb von 12 Monaten in sein Konto eingeloggt hat. Erfahrungsgemäß schauen viele Mitarbeitende nicht regelmäßig in das Zeitwertkonto. Dadurch kam es zu einer größeren Anzahl gesperrter Konten, mit der Folge, dass weder der Kontostand eingesehen noch das Passwort eigenständig geändert werden konnte. Um den damit verbundenen administrativen Aufwand zu reduzieren und nicht zuletzt die Nutzerfreundlichkeit zu erhöhen, wurde erwogen, die automatische **Sperrung der Konten** bei ausbleibender Nutzung auf 24 Monate statt einem Jahr einzustellen. Dem konnte ich ohne Weiteres zustimmen, da die automatische Sperrung keinen Einfluss auf die Geltungsdauer der Passwörter hat. Außerdem habe ich angeregt, perspektivisch eine **Zwei-Faktor-Authentifizierung** für die Zugänge oder am besten eine Koppelung mit dem System der E-Abrechnung (welches für die Verdienstbescheinigungen schon existiert) einzuführen.

3.2 Corona-Kontaktblätter an den Pforten

In Zeiten von Corona werden zur Nachverfolgung von Kontakten mehr Daten erhoben als das in Zeiten ohne Pandemie der Fall wäre. Daher habe ich beim Betriebsschutz Erkundigungen eingeholt, wie bezüglich der Speicherdauer und Vernichtung der **Kontaktblättern** verfahren wird, die **an den Pforten** ausliegen. Die Kontaktblätter werden vier Wochen aufbewahrt und anschließend in einen verschlossenen Metallbehälter gegeben, dessen Inhalt zur Vernichtung vorgesehen ist. Im Berichtszeitraum wurde die Verfahrensweise dann so umgestellt, dass die Blätter zunächst in einem Papiershredder vernichtet und erst anschließend der Entsorgung zugeführt wurden.

3.3 Corona-Schutzimpfungen der SWR-Mitarbeiter durch das DRK

Im Juni 2021 ergab sich auch für den SWR die Möglichkeit, seine Mitarbeiter unter Federführung des **Betriebsärztlichen Dienstes** an der **Arbeitsstelle** gegen das Coronavirus **impfen** zu **lassen**. Nach Evaluierung fiel die Wahl schnell auf das DRK, da die nötige Erfahrung vorhanden war und auch die vollständige Durchführung der Impfungen „aus einer Hand“ überzeugte. Für die Frage, wer für die zu verarbeitenden Daten verantwortlich ist, hatte ich die Zusammenarbeit mit dem DRK zu bewerten. Dabei spielte insbesondere eine Rolle, ob ein Fall der Auftragsverarbeitung vorlag, die den Abschluss eines entsprechenden Vertrages notwendig machen würde.

Die Zusammenarbeit gestaltete sich wie folgt: Das DRK war von der Terminplanung mit eigenem Terminplanungstool, über die Impfung selbst bis zur Dokumentation erster Ansprechpartner. Der SWR stellte ausschließlich die Infrastruktur, insbesondere die Gebäude, zur Verfügung. Außerdem informierte der SWR über das Impfangebot im Intranet und per Rundmail mit dem Link zum Terminbuchungstool. Bestellt wurde der Impfstoff über die Betriebsärzte, die das DRK bei den Impfungen unterstützte. Die **Beschäftigten** konnten sich dann **frei entscheiden**, ob sie das **Impfangebot im SWR** wahrnehmen wollten oder nicht. Da das Angebot freiwillig war und der SWR somit nur den Rahmen für die Impfungen bot, sah ich ausschließlich eine Verantwortlichkeit des DRK für die Datenverarbeitung. Daher war kein Auftragsverarbeitungsvertrag notwendig.

Ich habe aber angeregt, in die Vereinbarung aufzunehmen, dass das **DRK die Daten löscht**, wenn sie nicht mehr benötigt werden. Außerdem sollten die Daten der Mitarbeiter **nicht für andere Zwecke** verwendet werden dürfen, um ihnen beispielsweise an Weihnachten eine Spendenaufforderung oder Bitte, Mitglied beim DRK zu werden, zuzusenden. Des Weiteren wurde auch das Terminplanungstool von der IT-Sicherheit und mir überprüft. Alle Sicherheitsstandards wurden eingehalten, so dass eine sichere Datenübertragung gewährleistet war. Im Terminplanungstool waren ausschließlich diejenigen personenbezogenen Daten anzugeben, die für eine Zuordnung der Person absolut notwendig waren. Damit hatte ich keine Bedenken gegenüber einer Zusammenarbeit mit dem DRK. Unerfreulich war allerdings, dass es einzelne Beschäftigte gab, die sich nicht an die Regelungen halten wollten oder so weit gingen, DRK Mitarbeiter zu bedrohen.

3.4 Die Gretchenfrage nach dem Impfstatus

Im späten Herbst des Jahres war der überwiegende Teil der Mitarbeiterinnen und Mitarbeiter geimpft. Hier trat dann das Problem auf, ob der SWR als Arbeitgeber **nach dem Impfstatus fragen** darf. Die Tatsache, ob jemand geimpft ist oder nicht, ist eine sensible Information im Sinne von Art. 9 DSGVO. Allerdings können im Arbeitsverhältnis auch sensible Informationen verarbeitet werden, wie beispielsweise im Fall einer Krankmeldung oder die Frage nach einer Behinderung. Selbst nach Impfungen kann im Einzelfall gefragt werden, wie beispielsweise bei einem geplanten Auslandseinsatz in den Tropen.

Im vorliegenden Fall ging es darum, ob der Impfstatus im Hinblick auf COVID abgefragt werden darf. Nach den bisherigen medizinischen Erkenntnissen kann eine an COVID erkrankte Person andere Personen anstecken. Wenn also ein Mitarbeiter mit dieser Krankheit in den SWR kommt, kann er andere Mitarbeiter, aber auch Dritte (z.B. Interviewpartner) anstecken. Der SWR hat als Arbeitgeber jedoch eine **Fürsorgepflicht gegenüber allen Mitarbeitern** und gegebenenfalls haftet er gegenüber Dritten. Diese Fürsorgepflicht muss mit dem **berechtigten Interesse eines Mitarbeiters**, seinen Impfstatus nicht zu offenbaren, abgewogen werden. Im Rahmen dieser **Abwägung** ist vor allem die konkrete Tätigkeit des Mitarbeiters im SWR zu berücksichtigen. Wer beispielsweise in der Finanzverwaltung arbeitet und seine Arbeit im Home Office verrichtet, muss seinen Impfstatus nicht mitteilen. Anders sieht es aus, wenn dieser Mitarbeiter mit Wirtschaftsprüfern oder sonstigen Dritten so zusammenarbeiten muss, dass ein Kontakt erforderlich ist.

Bei Mitarbeiterinnen und Mitarbeitern, die per se **mit Dritten in Kontakt** kommen, weil sie zum Beispiel als Reporter arbeiten oder in der Produktion beschäftigt sind, sieht die Situation umgekehrt aus. Hier wird man grundsätzlich eine Mitteilung über den Impfstatus fordern dürfen. Daraus ergibt sich: Wenn es **für die konkrete Zweckbestimmung des Arbeitsverhältnisses notwendig** ist, dass ein Mitarbeiter mit anderen Mitarbeitern oder Dritten in Kontakt kommen muss, kann nach dem **Impfstatus gefragt** werden.

Die Problematik der **Weitergabe der Information**, also des Impfstatus, orientiert sich ebenfalls an der Zweckbestimmung: Diejenigen die wissen müssen, ob sie bestimmte Mitarbeiter einsetzen können, müssen auch wissen, ob diese geimpft (oder genesen) sind.

Für **Disponenten** wird dies normalerweise erforderlich sein, da sie Kenntnis darüber haben müssen, ob jemand geimpft ist oder nicht, damit eine entsprechende Einteilung vorgenommen werden kann. Da der Vorgesetzte im Regelfall für seinen Bereich verantwortlich ist und dessen Arbeitsfähigkeit sicherstellen muss, wird man auch ihm das Recht zubilligen müssen, vom Impfstatus zu erfahren. Er muss aber nicht wissen, mit welchem Impfstoff seine Mitarbeiterinnen und Mitarbeiter geimpft worden sind.

Die Daten zum Impfstatus dürfen aber in jedem Fall nicht ohne **Wissen des Mitarbeiters** gespeichert werden. Es ist ein Grundsatz des Datenschutzes, dass Betroffene über Daten informiert werden, die über sie gespeichert sind. Somit muss bereits bei der Erhebung und vor der Speicherung der Mitarbeiter aufgeklärt und informiert werden, was im Hinblick auf seine Daten geschieht, also insbesondere wer Zugriff hat.

Wenn Mitarbeiter **freiwillig** die Speicherung ihres Impfstatus wünschen, so sind sie ebenfalls darüber aufzuklären, wo dies geschieht beziehungsweise wer Zugriff darauf hat. Wenn ein so informierter Mitarbeiter dann einer Speicherung zustimmt, ist dagegen nichts einzuwenden. Diese Zustimmung zur Speicherung kann auch ein Mitarbeiter erteilen, der nach dem Zweck seines Arbeitsvertrages überhaupt nicht mit anderen Mitarbeitern oder Dritten in Berührung kommt (also beispielsweise der oben genannte "Finanzmitarbeiter" im Home Office).

Wie so oft macht ein Federstrich des Gesetzgebers ganze Bibliotheken und damit auch Rechtsstreitigkeiten zur Makulatur. Denn inzwischen wurde das **Infektionsschutzgesetz (IfSG) geändert** und § 28 b IfSG verpflichtet alle Arbeitgeber ihre Arbeitsstätten nur solchen Beschäftigten zugänglich zu machen, die geimpft, genesen oder entsprechend getestet sind. Das Gesetz schreibt darüber hinaus vor, dass die Arbeitgeber die Einhaltung dieser Verpflichtung durch Nachweiskontrollen täglich zu überwachen und regelmäßig zu dokumentieren haben. Zudem werden wie so oft Verstöße als Ordnungswidrigkeiten eingestuft.

3.5 Videokonferenzsystem Teams folgt auf Skype for Business

Die Coronapandemie hatte im SWR einen Digitalisierungsschub zur Folge und förderte **Videokonferenzlösungen**. Um die Arbeit in vielen Bereichen weiterhin überhaupt erledigen zu können, mussten digitale Lösungen gesucht und gefunden werden. So kamen zahlreiche neue Anwendungen zum Einsatz, die die standortübergreifende

Zusammenarbeit auch nach Corona deutlich verbessern werden. Dazu zählen insbesondere Telepräsenz-Lösungen, die einen kontaktlosen Austausch in der Pandemie überhaupt erst möglich gemacht haben. Auch zukünftig können dadurch viele Dienstreisen entfallen, die regelmäßig mit einem erheblichen Zeit- und Kostenaufwand verbunden und vor allem auch für unsere Umwelt belastend sind.

Seit dem 12. Juli 2021 wurde eine dieser Lösungen, die Anwendung **"Skype for Business"**, **im SWR deaktiviert** und ist damit nicht mehr verfügbar. An ihre Stelle tritt die Anwendung **„Teams“ von Microsoft**, die bereits seit einiger Zeit parallel genutzt werden konnte. Schließlich war von Anfang an geplant, Skype for Business nur als Übergangslösung einzusetzen. Mit der nahezu ausschließlichen Nutzung von Teams für Besprechungen und Konferenzen im SWR und der darin gegebenen Aufzeichnungsfunktion, mussten verbindliche Regelungen gefunden werden, um die Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter zu schützen. Denn das **Aufzeichnen von Besprechungen** stellt einen **Eingriff in die Persönlichkeitsrechte** der Teilnehmer dar und ist grundsätzlich untersagt.

Eine Ausnahme kann für Aufzeichnungen zu Informations- und Schulungszwecke gemacht werden, sofern eine **zwingende betriebliche Erforderlichkeit** gegeben ist. Dies bedeutet, dass es keine Alternativen gibt und bestimmte Anforderungen eingehalten werden.

Damit die Mitarbeiterinnen und Mitarbeiter über die Möglichkeiten des Einsatzes von Aufzeichnungen im Rahmen von „Teams“ informiert sind, wurden in Abstimmung mit mir Vorgaben formuliert und im Intranet veröffentlicht. Dort war dann zu lesen:

Was darf aufgezeichnet werden, wenn es zwingend betrieblich erforderlich ist?

- Schulungen, Webinare und Workshops
- Informationsveranstaltungen
- Präsentationen innerhalb einer Besprechung
- Live-Ereignisse

Was darf nicht aufgezeichnet werden?

- Grundsätzlich alle Besprechungen, die nicht unter die oben genannte Aufzählung fallen.
- Nicht zwingend betriebliche notwendige Besprechungen, wenn Teilnehmer*innen der Aufzeichnung schriftlich oder mündlich widersprechen.

Was ist bei einer Aufzeichnung zu beachten?

- Bei geplanten Aufzeichnungen ist diese schon in der Einladung zur Besprechung kenntlich zu machen.
- Wer die Videoschalte aufzeichnet, hat vor dem Start auf die Aufzeichnung im Besprechungschat hinzuweisen und den Teilnehmern die nötige Zeit einzuräumen, sich zu äußern und die Veranstaltung ggf. zu verlassen.
- Die Teilnehmer*innen einer nicht zwingend betrieblich notwendigen Besprechung müssen der Aufzeichnung im Besprechungschat zustimmen. Legen Sie hierzu im Vorfeld ein Wording oder Zeichen fest. Die Zustimmung muss bis zur Löschung der Aufzeichnung dokumentiert werden, z. B. durch einen Screenshot.
- Teilnehmer*innen, die prinzipiell einer Aufzeichnung zugestimmt haben, aber selbst nicht aufgezeichnet werden möchten, deaktivieren die Kamera und das Mikrofon.
- Nicht mehr benötigte Aufzeichnungen sind umgehend zu löschen. Es ist vorab über die geplante Dauer der Speicherung zu informieren.
- Vor der Weitergabe einer Aufzeichnung an Personen, die nicht Teil der Besprechung waren, werden die aufgezeichneten Teilnehmer*innen informiert.

Wessen Bilder und Töne dürfen aufgezeichnet werden?

- Protagonist*innen, z. B. Referent*innen, Trainingsleitungen, Moderator*innen usw.
- Teilnehmer*innen, die im Vorfeld auf die Aufzeichnung hingewiesen wurden und sich wissentlich aktiv an der Besprechung beteiligen wollen und hierbei bewusst für die Zeit ihres Beitrages ihr Kamera und Mikro aktiviert haben.

3.6 Ein elektronisches Behördenpostfach (beBPo) auch für den SWR

Die neuen gesetzlichen Anforderungen **im elektronischen Rechtsverkehr** betreffen ab dem 1. Januar 2022 auch den SWR. Insbesondere das Justitiariat und der Beitragsservice sind davon betroffen. Denn ohne Nutzung des besonderen elektronischen Behördenpostfaches (ERVV) gelten Dokumente, die an ein Gericht übermittelt werden, als nicht oder verspätet zugegangen. Deshalb braucht auch der SWR ein elektronisches Behördenpostfach. Als einer der wenigen Anbieter, die über eine notwendige Zulassung der Justiz verfügen, wurde die Lösung der Firma Governikus in Betracht gezogen. Diese sieht eine **E-Mail-Anbindung an ein elektronisches Behördenpostfach** als Software as a Service (SaaS) vor. Dies bedeutet, dass die Software und die dafür erforderliche IT-Infrastruktur bei Governikus betrieben und vom SWR ausschließlich als Dienstleistung genutzt wird. Da es bei dieser Art von Dienstleistung **regelmäßig** zum **Austausch personenbezogener Daten** kommt, führte ich eine Prüfung der Verarbeitung durch. Infolgedessen war ein Vertrag zur Auftragsvereinbarung nach Art. 28 DSGVO zu schließen und geeignete technische und organisatorische Maßnahmen (TOMs) vorzusehen, die die Sicherheit der Daten nach Art. 32 DSGVO gewährleisten. In dem AV-Vertrag von Governikus ist geregelt, dass die Daten ausschließlich in Deutschland, der EU oder dem EWR verarbeitet werden. Für eine Verarbeitung außerhalb dieses Gebiets, bedarf es der ausdrücklichen Zustimmung des SWR und überdies der Erfüllung der besonderen gesetzlichen Voraussetzungen nach Art. 44 ff DSGVO. Somit bestehen im Hinblick auf den **Ort der Datenverarbeitung** und das damit verbundene Datenschutzniveau **keinerlei Bedenken**. Der von Governikus vorgelegte AV-Vertrag erfüllt in jeder Hinsicht die gesetzlichen Anforderungen der DSGVO und ist auch vorbildlich ausgestaltet. Daher konnte ich dem Vorhaben ohne Weiteres zustimmen.

3.7 Das Ende einer unendlichen Geschichte

Ich hatte in den beiden letzten Tätigkeitsbericht (2019 unter Ziff. 3.1; 2020 unter Ziff. 3.6) berichtet, dass der SWR versucht hat, alle Mitarbeiterinnen und Mitarbeiter **auf die Vertraulichkeit** entsprechend den Vorgaben der DSGVO zu **verpflichten.** Erst am 4. März 2021, also fast **drei Jahre** nachdem die entsprechende Erklärung nebst Merkblatt zur Unterschrift an die Mitarbeiterinnen und Mitarbeiter versandt worden ist, wurde mir

gemeldet, dass die letzten elf Mitarbeiter die **Verpflichtung auf die Vertraulichkeit** unterschrieben haben.

3.8 Erste Hilfe Verbandskästen datenschutzkonform gestalten

Trotz allen Vorsichtsmaßnahmen geschehen immer wieder Arbeitsunfälle. Deshalb schreibt der Gesetzgeber vor, dass **frei zugängliche Verbandskästen** vorhanden sein müssen, in denen sich ein sog. „**Verbandbuch**“ befindet. Darin sind die jeweiligen Erste-Hilfe-Leistungen zu dokumentieren. Denn die von den Unfallversicherungsträgern aufgrund **§ 15 SGB VII** unter Mitwirkung der Deutschen Gesetzlichen Unfallversicherung (DGUV) „als autonomes Recht“ erlassenen **Unfallverhütungsvorschriften** schreiben in „Grundsätze der Prävention“ in § 24 Abs. 6 vor, dass ein Unternehmer dafür zu sorgen hat, „dass **jede Erste-Hilfe-Leistung dokumentiert** und diese Dokumentation fünf Jahre lang verfügbar gehalten wird.“ Sofern diese Dokumentation noch immer in einem in der Praxis vorhandenen „kleinen grünen Büchlein“ erfolgt, ist hier eine Änderung vorzunehmen und stattdessen der von den Berufsgenossenschaften zur Verfügung gestellte **Meldeblock mit Einzelformularen** zu verwenden. Danach ist das nach einer Hilfeleistung ausgefüllte Formular bei der zuständigen Stelle abzugeben und darf nicht (wie früher das grüne Büchlein) weiter im Verbandskasten aufbewahrt werden.

3.9 Kein öffentlich-rechtliches Aushängeschild: Der Landesrechnungshof versucht es einfach

Der **Landesrechnungshof** hat die Aufgabe, Prüfungen, insbesondere zur Wirtschaftlichkeit des Handelns des SWR vorzunehmen. Dieses Mal war geplant, einen Schwerpunkt auf die betriebliche Altersvorsorge (inklusive Vorruhestand) zu legen. Dazu sollten aber nicht nur die einschlägigen rechtlichen Regelungen vorgelegt werden, sondern man wollte auch eine **Liste aller Versorgungsempfänger, Vorruheständler** bzw. **Witwen und Witwern**. Zudem sollte der Zugriff auf die Daten von bestimmten einzelnen Personen ermöglicht werden und man wollte **im Gehaltssystem recherchieren** können. Damit wären die **kompletten Verdienstabrechnungen** aller Mitarbeiterinnen und Mitarbeiter sowie die Zahlungen aller Versorgungsfälle jeweils im Einzelfall einzusehen gewesen. Als ich eher zufällig davon erfahren habe, habe ich das Justitiariat und die Verwaltungsdirektion darauf hingewiesen, dass für den Zugriff auf sensible Personaldaten

eine **bestimmte und normenklare Rechtsgrundlage nötig** sei. Eine allgemeine **Aufgabenbeschreibung** wie sie das Landesrechnungshofgesetz vorsieht, sei **nicht ausreichend**. Es können zwar Informationen angefordert werden, es bestehe aber keine Rechtsgrundlage für den Zugriff auf Einzeldaten. Nach § 35 Abs. 5 SWR Staatsvertrag i.V.m. § 111 Landeshaushaltsordnung Baden-Württemberg sind die Regelungen zur Prüfung der Haushalts- und Wirtschaftsführung anzuwenden. Doch diese Normen geben **keine Ermächtigungsgrundlage** ab, auf **personenbezogene Daten einzelner Beschäftigter** zugreifen zu dürfen. Ich habe auf das Erfordernis einer konkreten Rechtsgrundlage schon im Hinblick auf das damalige datenschutzwidrige Verlangen der KEF hingewiesen, Daten konkreter einzelner Personen einsehen zu wollen (vgl. hier Ziff. 5.5 sowie Ziff. 3.11 im 10. TB 2016-2017).

Nach monatelangem Hin und Her hat der Rechnungshof dann überraschend bei der Verwaltungsdirektion angerufen und mitgeteilt, dass er auch **mit anonymisierten oder geclusterten Daten zufrieden** sei. Das konkrete Problem ist damit erledigt, doch es bleibt ein schaler Nachgeschmack, dass eine **staatliche Behörde versucht** hat, **personenbezogene Daten ohne datenschutzrechtliche Rechtsgrundlage zu erheben**.

3.10 Ein gelungener Jahresabschluss

In der Vergangenheit gab es immer wieder Irritationen mit den Wirtschaftsprüfern. Dabei ging es mir ausschließlich darum, dass **mit den erhaltenen Daten** der Mitarbeiter **ordnungsgemäß umgegangen** wird. Die Daten dürfen **nicht für andere Zwecke** verwendet und es muss für deren Sicherheit gesorgt werden. Außerdem sind die Daten frühzeitig zu löschen bzw. zu anonymisieren. Bei den Tätigkeiten der sogenannten **Berufsgeheimnisträger**, z. B. Steuerberater oder Wirtschaftsprüfer, handelt es sich im Datenschutz um eine **Inanspruchnahme fremder Fachleistungen** bei einem **eigenständigen Verantwortlichen**. Doch auch wenn damit kein Fall der Auftragsverarbeitung vorliegt und somit kein Auftragsverarbeitungsvertrag zu schließen ist, müssen dennoch vertragliche Regelungen vorliegen, die die genannten Mindestanforderungen beschreiben. Erfreulicherweise hat die vom SWR beauftragte Wirtschaftsprüfungsgesellschaft Verträge mit einer Regelung zum Datenschutz vorgelegt. Danach erfolgt die Verarbeitung personenbezogener Daten unter **strikter Zweckbindung**

und enthält **Löschfristen**, die an den **gesetzlichen Aufbewahrungsvorschriften** ausgerichtet sind. Es fehlten lediglich Angaben zur Datensicherheit. Ich habe daher veranlasst, dass die Anforderungen des SWR an die technischen und organisatorischen Maßnahmen zur Datensicherheit (TOMs) der Wirtschaftsprüfungsgesellschaft vorgelegt und damit unterzeichnet werden konnten.

3.11 Datenschutz im Justitiariat

Arbeitsrechtliche Streitigkeiten sind mehr oder minder das tägliche Brot einer Rechtsabteilung. Dabei müssen oft sensible Daten von Mitarbeitern verarbeitet werden. Auch die Pandemie machte davor nicht Halt. Was einen Mitarbeiter im Rahmen eines Arbeitsgerichtsprozesses aber erzürnte, war die Tatsache, dass der im Home Office arbeitende Jurist ein dienstliches Telefax von seinem privaten Gerät zu Hause aus an das Arbeitsgericht sandte, das als Kennung seinen und den Namen seiner Ehefrau trug. Ich habe im Rahmen seiner Beschwerde im September die entsprechenden Ermittlungen beim Justitiariat in Mainz vorgenommen. Dort wurde mir erklärt, dass jetzt zukünftig ein Faxversand nicht mehr über private Geräte erfolgt, sondern mit MS Office 365 elektronisch. Außerdem arbeitet man auch an einer speziellen datenschutzrechtlichen Regelung für die Rechtsabteilung. Im Übrigen sollen die Regelungen des neuen Tarifvertrages Flex-AO, welcher auch das Home Office regelt, zugrunde gelegt werden (zum Beispiel auch im Hinblick auf Kontrollen, die allerdings von den Justitiarinnen für die Mitarbeiter der Rechtsabteilung für nicht geboten gehalten werden).

3.12 Zukunftsmusik: Der Tarifvertrag zur flexiblen Gestaltung des Arbeitsortes im SWR (TV FlexAO–SWR)

Der SWR hat lange mit den Gewerkschaften über einen „Tarifvertrag zur flexiblen Gestaltung des Arbeitsortes im SWR“ verhandelt. Nach Zustimmung des Verwaltungsrates wird er zum 1. April 2022 in Kraft treten. Dem Datenschutz ist (zusammen mit der IT-Sicherheit) ein eigener Abschnitt gewidmet, für den auch ich Anregungen gegeben habe.

4 Datenschutz beim ARD ZDF Deutschlandradio Beitragsservice

4.1 Grundlagen zum Rundfunkbeitrag

Die Rundfunkfinanzierung wurde zum 1.1.2013 von der Gerätegebühr auf die Erhebung eines **Rundfunkbeitrags** umgestellt. Danach wird im Privatbereich pro Wohnung ein Beitrag erhoben, 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) in Köln durch den „**ARD ZDF Deutschlandradio Beitragsservice**“ als zentrales Rechenzentrum aller Rundfunkanstalten für den Beitragseinzug. Nur noch ganz spezielle Sachverhalte werden von den im Abbau begriffenen dezentralen Beitragsabteilungen in den einzelnen Landesrundfunkanstalten betreut.

Für die **datenschutzrechtliche Kontrolle** dieses Zentralen Beitragsservice 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 (vgl. auch die Anmerkungen 23 bis 29 in § 28 HDSIG in dem von Roßnagel herausgegebenen Datenschutz-Kommentar im Nomos-Verlag). Denn die Landesdatenschutzbeauftragten wirken damit als staatliche Fremdkontrollorgane in die Rundfunkanstalten hinein, und zwar insbesondere in den 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 7,3 Mio. privaten **Rundfunkbeitragskonten** im **Sendegebiet 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 (vgl. auch Herb, VBlBW 2020, S. 492 ff.).

Routinemäßige Datenschutzaufgaben im Bereich des Beitragseinzugs werden gemäß § 11 Abs. 2 Rundfunkbeitrags-Staatsvertrag (RBStV) von der internen Datenschutzbeauftragten des Zentralen Beitragsservice vor Ort in Köln wahrgenommen. Sie ist oft erste Ansprechpartnerin bei Datenschutzbeschwerden beim Beitragsservice. 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 sowie der Verwaltung der rund 45,4 Millionen Beitragskonten zuständig.

Der Anteil der **SWR-Beitragszahler** am Gesamtaufkommen liegt bei etwa 7,3 Mio. privaten und ca. 694.000 nicht-privaten (also geschäftlichen) Rundfunkbeitragskonten bei ca. 17,6 % 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.

4.3 Erlass und Widerspruch von Bescheiden unter einem Dach?

Beim Einzug von Rundfunkbeiträgen (ehemals Rundfunkgebühren) werden Beitragsbescheide, aber auch Beitragsbefreiungen erlassen. Die Bescheide werden vom Zentralen Beitragsservice (ZBS, ehemals GEZ) im Namen der jeweiligen Landesrundfunkanstalt erlassen. In der Vergangenheit haben die Landesrundfunkanstalten die **Widersprüche gegen die Bescheide** selbst bearbeitet. Im Laufe der Zeit sind aber immer mehr Landesrundfunkanstalten dazu übergegangen, die Widerspruchsbescheide vom ZBS erstellen zu lassen. In der Folge wurde **beim ZBS eine Organisationseinheit** gebildet, die ausschließlich für den **Erlass von Widerspruchsbescheiden** zuständig und bei der Rechtsabteilung des ZBS angesiedelt war. Im Januar 2021 wurde nun die Widerspruchsabteilung in den Geschäftsbereich eingegliedert, der auch die Ausgangsbescheide erlässt. Ich habe erhebliche Zweifel, dass dies den Vorgaben der VwGO entspricht, denn Sinn und **Zweck des**

Widerspruchsverfahrens (sogenanntes Vorverfahren nach § 68 VwGO) ist eine Überprüfung durch eine andere, von der Behörde, die die Ausgangsbescheide erlässt, **unabhängige Stelle**. Auch die Aufgabenzuteilung in zwei voneinander getrennte Teams innerhalb dieses Geschäftsbereichs kann meine Zweifel an der Fragwürdigkeit dieser Konstellation nicht zerstreuen.

4.4 Meldedatenabgleich

Der letztmals im Mai 2018 durchgeführte **Meldedatenabgleich** ist jetzt **als regelmäßiges Instrument** des Beitragsservice in § 11 Abs. 5 Rundfunkbeitrags-Staatsvertrag (RBStV) vorgesehen. Der **nächste Abgleich** wird im Jahre **2022** stattfinden. Wie bereits in den letzten Tätigkeitsberichten vermeldet, gab es dazu bislang kaum datenschutzrechtliche Beschwerden oder Vorkommnisse (vgl. zu den Beschwerden auch Ziff. 6.1.1).

4.5 Dauerhaft Home Office beim Beitragsservice möglich (und sinnvoll?)

Nach Ausbruch der Corona-Pandemie hat der **Zentrale Beitragsservice (ZBS)** in Köln die Mitarbeiterinnen und Mitarbeiter soweit möglich ins Home Office gesandt. Dazu wurden auch entsprechende Regelungen getroffen. Da die Erfahrung mit diesem neuen Instrument positiv waren (angeblich höhere Produktivität und niedriger Krankenstand), hat der ZBS ab 1. Juli 2021 **dauerhaft** und unabhängig von der Pandemiesituation die **Arbeit im Home Office zugelassen**. Dies ist dann kritisch zu sehen, wenn dadurch die Mitarbeiter den Zugriff auf den gesamten Datenbestand der über 45,4 Mio. erhalten.

Für die Arbeit im Home Office dürfen nur dienstliche Geräte genutzt werden. Der Einsatz privater Geräte ist verboten (mit Ausnahme der Nutzung von Peripheriegeräten und Privatgeräten zur Teilnahme an Videokonferenzen). Ebenso ist die private Nutzung von Internet und E-Mail verboten. Telefongespräche sollen vorzugsweise ebenfalls über dienstliche Geräte erfolgen. Verboten ist insbesondere die Nutzung privater Endgeräte im Bereich der Kommunikation mit Beitragsschuldnern. Die Vorgaben zum Datenschutz und der Informationssicherheit wurden überarbeitet und stellenweise verschärft. Der ZBS beabsichtigt, diese ergänzenden Regelungen von jedem Mitarbeiter, der im Home Office arbeiten will, unterschreiben zu lassen.

4.6 Neuer Inkasso-Dienstleister

Hatten die staatlichen Vollstreckungsorgane keinen Erfolg bei der Beitreibung einer **Forderung aus dem Rundfunkbeitragseinzug**, so ist in der Vergangenheit die Firma Creditreform in Mainz beauftragt worden, die Schuldner nochmals anzuschreiben, um Zahlungen zu erreichen. Dies hat jahrelang reibungslos funktioniert und weil Mainz im Sendegebiet des SWR liegt, habe ich dort regelmäßig eine Datenschutzkontrolle (auch im Auftrag der anderen Rundfunkanstalten) vorgenommen. Jetzt ist eine neue **Ausschreibung** durch den Beitragsservice erfolgt. Den Zuschlag erhielt die Firma Paigo GmbH, die früher „infoscore Forderungsmanagement GmbH“ hieß und als Teil der Firmengruppe „Arvato Financial Solutions“ zum Bertelsmann-Konzern gehört. Da die Firma im Auftrag des Beitragsservice (letztlich aber aller Landesrundfunkanstalten) tätig ist, wurde ein **neuer Auftragsdatenverarbeitungsvertrag** abgeschlossen sowie ein umfangreiches, 52-seitiges (ohne Anlagen) “Verfahrenshandbuch über die Inkassodienstleistungen der Paigo GmbH für den Beitragsservice“ verfasst. Es regelt detailliert die Anforderungen, womit kein Zweifel besteht, dass ein Auftragsdatenverarbeitungsverhältnis vorliegt.

4.7 EUDAGO

Das gewaltige Projekt EUDAGO des Beitragsservice, also die **finale Umsetzung der EU-Datenschutz-Grundverordnung** (DSGVO), konnte 2021 abgeschlossen werden.

Vor der Geltung der DSGVO bestand nach den Datenschutzgesetzen auch die Möglichkeit, statt einer Löschung eine Sperrung vorzunehmen, wenn die Löschung einen unverhältnismäßig hohen Aufwand erforderte (vgl. § 20 Abs. 3 Nr. 3 BDSG alte Fassung). Diese Möglichkeit ist mit Geltung der DSGVO weggefallen, womit auch eine Lösung gefunden werden musste, nicht nur eine logische Löschung, sondern auch eine **physische Löschung** vorzunehmen. Dies bedeutete eine gewaltige Herausforderung. Denn das seit Gründung der GEZ existierende Großrechnersystem, welches effizient war und die Bearbeitung der inzwischen auf über 45,4 Millionen angewachsenen Teilnehmerkonten im Online-Verfahren erlaubte, musste umgebaut werden. Das Problem war dabei, dass fast alle gespeicherten Informationen einen Buchhaltungsbezug haben und deshalb bei einer Löschung Fehler im Teilnehmerkonto hätten entstehen können. Im Abschlussbericht konnte jedoch festgestellt werden, dass die Löschungen reibungslos

verlaufen sind und inzwischen auch die regelmäßigen Löschungen mit ihren unterschiedlichen Löschfristen unter Berücksichtigung der neueren Rechtsentwicklung auf die neue Rechtslage im System erfolgreich verankert werden konnten.

4.8 Kontaktdaten der Datenschutzbeauftragten des Beitragsservices

Bislang war die Datenschutzbeauftragte des Beitragsservices unter datenschutz@beitragsservice.de erreichbar. Diese Möglichkeit wurde abgeschaltet. Die Datenschutzbeauftragte ist nicht mehr per E-Mail erreichbar, was im digitalen Zeitalter, das durch die Pandemie einen beschleunigten Ausbau erfährt, nicht verständlich ist. Unter https://www.rundfunkbeitrag.de/datenschutz/datenschutzkontaktformular/index_ger.html wird zwar ein Kontaktformular angeboten, doch dieses ist missverständlich. Weil es dort heißt: „Wir beantworten Ihre Fragen zum Datenschutz“ und dies auch durch den Verantwortlichen selbst erfolgen könnte und deshalb nicht der direkte Weg zur Datenschutzbeauftragten aufgezeigt wird.

Die Begründung für die Abschaltung, es seien zu viele beitragsrechtliche statt datenschutzrechtlicher Fragen eingegangen und zudem könne man den Arbeitsaufwand nicht bewältigen, überzeugt nicht: Abgesehen davon, dass nach Art. 37 Abs. 7 DSGVO die Kontaktdaten der Datenschutzbeauftragten zu veröffentlichen wären, muss nach Art. 38 Abs. 2 DSGVO der Verantwortliche die zur Aufgabenerfüllung erforderlichen Ressourcen zur Verfügung stellen. Auch bei den Rundfunkbeauftragten für den Datenschutz gehen „sachfremde“ Fragen und Beschwerden ein, die aber dann eben an die entsprechenden Stellen weitergeleitet werden (siehe unten Ziff. 6.1.2 und 6.1.3).

5 Datensicherheit im SWR

Die Notwendigkeit, **Vorkehrungen gegen Hackerangriffe** zu treffen, ist inzwischen bei allen Unternehmen und Behörden fast zum Routinegeschäft geworden. Denn nach wie vor gibt es auch beim SWR praktisch täglich Attacken auf die Rechner. Notwendig ist es deshalb, dem Stand der Technik entsprechende Maßnahmen zu ergreifen (Art. 32 DSGVO).

5.1 Achtung: Gefälschte Mails mit Kalendereinträgen

Im Frühjahr 2021 gingen vermehrt **gefälschte E-Mails mit Kalendereinträgen** im SWR ein. In den Mails befanden sich Einladungslinks zu angeblich stattfindenden Besprechungen. Die IT des SWR machte auf das Problem aufmerksam und sensibilisierte die Mitarbeiterinnen und Mitarbeiter. Es genügte jedoch nicht, nur die Einladungsmail zu löschen, da die Kalendereinträge ansonsten weiter Bestand gehabt hätten. Dementsprechend wurde empfohlen, bereits in der Vorschau der Einladung die Option „ablehnen“ und „keine Antwort senden“ auszuwählen. Nur damit sind Einladungsmail und Kalendereintrag entfernt. Weiter wurde darauf hingewiesen, keinesfalls einen der Links anzuklicken, weder in der Mail noch im Kalendereintrag.

5.2 Verschlüsselung von Daten statt Faxversand

Der **Vergütungs- und Honorarservice** im SWR hat bislang seine **Meldungen per Fax** an einen **Dienstleister** in Nürnberg übermittelt. Im Berichtszeitraum stellte sich dann heraus, dass die Übermittlung nicht zuverlässig funktionierte, obwohl der Absender eine Versand- und Zustellbestätigung erhalten hatte. Auch eine intensive Schnittstellenüberprüfung konnte keine Abhilfe schaffen. Deswegen wurde der **Versand per E-Mail** mit Anhängen in Betracht gezogen. Die DSGVO fordert bei der Sicherheit der Verarbeitung personenbezogener Daten, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Um die Daten sicher übertragen zu können, bedarf es daher einer Inhalts- oder Transport-Verschlüsselung. Bei einer **Inhaltsverschlüsselung** (Ende-zu-Ende) werden die Standardprotokolle S/MIME und OpenPGP sowie die Microsoft Rights Management Services (RMS) empfohlen. Bei der **Transportverschlüsselung** ist das **Standardprotokoll TLS** (ehemals SSL) gebräuchlich. Der Dienstleister bot dem SWR das TLS-Verfahren für die Übermittlung von Daten an. Da nach dem Bundesamt für Sicherheit

in der Informationstechnik (BSI) eine TLS-Verschlüsselung erst ab der Version 1.2 zuverlässig ist, habe ich die zuständigen Stellen SWR gebeten, darauf zu achten. Gegenwärtig wird nun diese Version 1.2 eingesetzt.

5.3 SWR-IT-Sicherheitskonferenz

IT-Sicherheit und Datensicherheit unterscheiden sich dadurch, dass es sich bei Datensicherheit um personenbezogene Daten handeln muss, während die IT-Sicherheit weitergehend alle Komponenten erfasst. Da jedoch in praktisch allen Systemen personenbezogene Daten gespeichert werden und ein Ausfall der Systeme auch die Rechte von betroffenen Personen verletzen kann, ist der Unterschied in der Praxis regelmäßig ohne Bedeutung. Der Rundfunkbeauftragte für den Datenschutz des SWR ist deshalb auch Mitglied der mindestens jährlich stattfindenden **SWR-IT-Sicherheitskonferenz**.

5.4 Penetrationstest

Auch im Jahre 2021 wurde wieder über die RBT, die Arbeitsgemeinschaft Rundfunk-Betriebstechnik von ARD, ZDF und Deutschlandradio, ein **Penetrationstest**, also quasi ein simulierter Angriff durchgeführt. **Schwachstellen**, welche eine Übernahme von Systemen oder Anwendungen des SWR ermöglichen würden, wurden nicht gefunden. Kleinere Schwachstellen wie eine veraltete Software wurden beseitigt.

5.5 Datenerhebung ohne Rechtsgrundlage durch die KEF

Der „Kommission zur Überprüfung und Ermittlung des Finanzbedarfs der Rundfunkanstalten“ (KEF) obliegt es, den allgemeinen Finanzbedarf der Rundfunkanstalten fachlich zu überprüfen und zu ermitteln. Sie darf dazu zwar Auskünfte einholen, eine **Ermächtigung** oder Befugnis, **personenbezogene Daten** zu erheben, **fehlt** nach wie vor (vgl. bereits Ziff. 3.11 im 10.TB 2016-2017).

5.6 Und nochmals Clubhouse, die App für Hörfunk-Talkshows

Ich hatte bereits im letzten Tätigkeitsbericht (Ziff. 2.1) über **Clubhouse**, die datenschutzrechtlich problematische App berichtet. Jetzt wurde Ende Juli 2021 gemeldet, im Darknet sei eine gigantische Sammlung von **3,8 Milliarden Handy- und**

Festnetznummern zu „kaufen“. Betroffen wären dann nicht nur alle Nutzer der Audio-App Clubhouse, sondern auch deren sämtliche Kontakte, weil die App regelmäßig die digitalen Telefonbücher ihrer Mitglieder herunterlädt.

5.7 Kurz vor Weihnachten: Die Log4j-Sicherheitslücke

Die **Programmiersprache Java** wird zum Betrieb von Servern genutzt wird. Hier wurde kurz vor Weihnachten eine **Schwachstelle** erkannt, die zu einer massiven Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geführt hat. Die Java-Bibliothek Log4j protokolliert diverse Ereignisse im Server-Betrieb wie den Befehl, Kontakt zum Server des Angreifers aufzunehmen, von diesem einen Java-Code entgegenzunehmen und diesen auszuführen. Wenn dies einem Angreifer bekannt wird, kann er **Schadprogramme** auf den Server von Online-Diensten **platzieren**. Im Extremfall können **Unternehmen** vollständig **übernommen werden**. Nachdem im Netz eine Art Bedienungsanleitung (Proof-of-Concept) kursiert, um die Schwachstelle auszunutzen, hat das BSI die Lage als extrem kritisch eingeschätzt und daher die Cyber-Sicherheitswarnung der Warnstufe Rot veröffentlicht. Da die Anwendungen weltweit verbreitet sind, sind neben Apple, Twitter, Amazon, Tesla auch Behörden sowie der SWR betroffen. Das Ausmaß der Gefährdung lässt sich nach Einschätzung des BSI bislang noch nicht abschließend feststellen. Zum Schutz riet das BSI zunächst, Updates einzuspielen, sobald diese für die einzelnen Produkte zur Verfügung stehen. Doch die zunächst durchgeführten Updates waren letztlich nicht erfolgreich, da mit der neuen Version 2.15.0 bereits eine andere Schwachstelle zu Tage getreten ist. Nötig sind deshalb ständige Updates.

Beim SWR wurde zur Koordinierung der Sicherungsmaßnahmen und zur Prüfung und Sicherung der Server eine **Task Force eingerichtet**. Ein Sicherheitsvorfall wurde bislang nicht festgestellt. Ein Restrisiko bleibt jedoch, weil in der Programmverbreitung teilweise sehr alte Systeme zum Einsatz kommen, für die es keine Patches gibt. Außerdem ist die Erkennung von Cyberangriffen schwierig. Die in der Task Force vereinten Bereiche stellten auch über die Weihnachtsfeiertage eine freiwillige Erreichbarkeit sicher, um im Notfall angemessen und koordiniert reagieren zu können.

5.8 Datensicherheit im SAP Projekt durch Security Audit Logs

Ich hatte bereits im 13. TB unter Ziff. 3.1 über die ARD-weite SAP-Prozessharmonisierung berichtet. Bei diesem riesigen **SAP-Gesamtprojekt** mit 29 Einzelprojekten müssen auch **Aspekte der Datensicherheit** betrachtet werden. Das SAP Security Audit Log (SAL) bildet das Kernstück der SAP-Sicherheitsstrategie. Das SAL protokolliert alle sicherheitsrelevanten Protokoll-Einträge von falscher Passwort-Eingabe über externe *RFC-Aufrufe** bis hin zu Manipulationen an Transaktionen via Debugger in einem Protokoll auf dem SAP-Server (Standort in Deutschland).

**RFC (Remote Function Call) ist ein Begriff aus dem Umfeld der SAP-Software und bezeichnet Verfahren, mit denen Funktionen in einem entfernten System aufgerufen werden.*

Wenn das Security-Audit-Log aktiviert wird, werden Aktionen aufgezeichnet, die für die Verfolgung als relevant eingestuft werden. In Form eines Audit-Analysereports ist der Zugriff auf und die Auswertung dieser Informationen bzw. personenbezogenen Daten möglich. Nach dem **Prinzip der Datensparsamkeit** werden nur die für die Einhaltung der Schutzziele (Verfügbarkeit, Authentizität, Integrität, Vertraulichkeit, Verbindlichkeit) notwendigen Daten protokolliert. **Security Audit Logs** werden grundsätzlich **nach 3 Monaten gelöscht**, es sei denn, im Zeitraum der Protokollierung kam es zu Sicherheitsvorfällen. Dann gilt eine verlängerte Aufbewahrung von 2 Jahren. Dies lässt sich nur dadurch rechtfertigen, dass es inzwischen vermehrt Cyber-Angriffe ergibt, welche vorab über einen längeren Zeitraum vorbereitet werden.

6 Auskunftsersuchen und Beschwerden

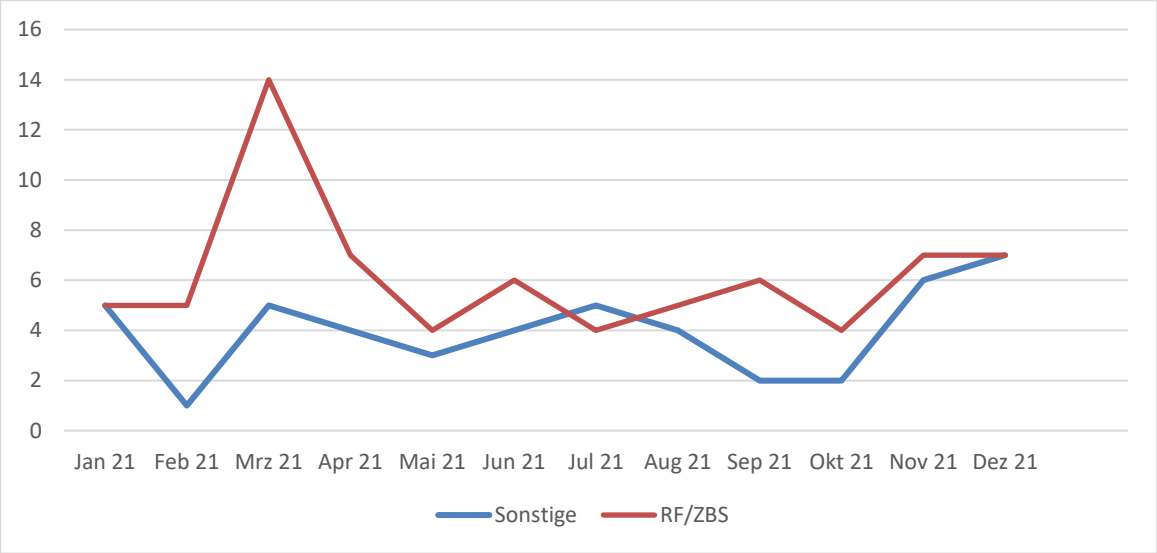
Auch in der Corona Pandemie werden Auskunftsansprüche geltend gemacht und gehen Beschwerden über vermeintliche Datenschutzverstöße ein. Dies gilt sowohl für die Eingaben beim SWR (Ziff. 6.1) als auch beim Zentralen Beitragsservice (Ziff. 6.2).

6.1 Beim SWR eingegangene Auskunftsersuchen und Beschwerden

Die **Beschwerden und Auskunftsersuchen**, die direkt an mich bzw. den SWR gehen werden **immer komplexer und schwieriger** zu bearbeiten. 2021 ist zwar die nominelle Anzahl gesunken, doch waren sie vielfältiger, differenzierter und **im Einzelfall**

schwieriger zu bearbeiten und zu beantworten. Auch in der Pandemiesituation kommen viele der Beschwerden noch per Post und müssen auch mit der klassischen Post beantwortet werden. Eine Beantwortung im Home Office war in der überwiegenden Zahl der Fälle nicht möglich, sondern es musste vor Ort, **im Funkhaus des SWR** gearbeitet werden. Da der Datenschutzbeauftragte dort seit März 2020 in ein abgelegenes Untergeschoss abgeschoben worden ist, hatte dies zumindest den Vorteil, dass praktisch keine Kontakte mit anderen (bis auf die Poststelle) stattfanden.

Insgesamt **117 Beschwerden und Auskunftsersuchen im Jahr 2021** waren zu bearbeiten (gegenüber 166 Beschwerden im Jahre 2020). Die beiliegende Übersicht zeigt den **Eingang im Monatsverlauf** des Jahres **2021**:



6.1.1 Direkteingaben zum Rundfunkbeitragseinzug

Von den insgesamt 117 Beschwerden, die bei mir im Jahr 2021 eingingen, betrafen **70** den **Rundfunkbeitragseinzug**, wobei oftmals auch weitere vermeintliche Datenschutzverletzungen angesprochen oder Statements abgegeben wurden.

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 oder Daten seien zu Unrecht erhoben oder zu Unrecht gespeichert worden. Es wird immer schwieriger, den Beschwerdeführern klarzumachen, dass zuerst die beitragsrechtlichen Fragen zu klären

sind. Besonders schwierig ist dies bei den knapp ein Dutzend Petenten, die sich auch in diesem Jahr als **Reichsbürger** zu erkennen gaben.
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, **Auskunftsersuchen** im Hinblick auf den Rundfunkbeitragseinzug **innerhalb von 78 Stunden** zu beantworten, konnte 2021 trotz Pandemie fast immer erreicht werden.

6.1.2 Sonstige Direkteingaben beim Rundfunkdatenschutzbeauftragten

Die **Eingaben und Beschwerden** ohne jeglichen Bezug zum Rundfunkbeitragseinzug sind mit **47** nach wie vor sehr hoch. Es ist eine **steigende Tendenz** zu verzeichnen. Die Mehrzahl dieser Petenten zeichnet sich durch eine **kritische Begleitung der Programme** des SWR aus. Datenschutz- und **Programmkritik** erfolgte insbesondere bei folgenden Internet-Aktivitäten:

- Oft wurden angebliche formale **Verstöße auf den Webseiten oder** im Hinblick auf **Cookies** gerügt, wobei sich hier im Regelfall nach Erklärungen und Erläuterungen eine Erledigung erzielen ließ. Das **Tracking** der Seiten (siehe dazu auch oben Ziff. 2.6 und 2.9) wird zunehmend gerügt, obwohl nur eine anonymisierte Auswertung erfolgt und in den meisten Fällen ein Opt-Out besteht.

- Die **Löschungsbegehren** gegenüber gesendeten oder geposteten Beiträgen in Programmen bzw. SWR-Webseiten nehmen langsam, aber kontinuierlich zu. Auch wenn zunächst eine Einwilligung zur Verwendung von Aussagen oder Bildern gegeben worden ist, widerruft man diese später.

- Die Gendersternchen (**) geben immer wieder Anlass zur Kritik.

- Wie in den vergangenen Jahren, wurde die **Präsenz auf Drittplattformen bzw.** in den **sozialen Medien** gerügt. Viele Petenten fanden kein Verständnis dafür, dass der SWR sich mit „Datenkraken“ wie **Facebook**, **Instagram** oder **TikTok** einlässt oder **WhatsApp** als Kommunikationskanal anbietet. 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; das Gleiche gilt für WhatsApp. Allerdings ist die rechtliche Bewertung aufgrund der durch das Medienprivileg geschaffenen Ausnahmen schwierig.

6.1.3 Programmbeschwerden an datenschutz@swr.de

Immer mehr Personen lassen ihren **Ärger über den Beitragsservice und** zunehmend auch **über das Programm** freien Lauf, indem sie an die E-Mail-Adresse *datenschutz@swr.de* schreiben. Ob dies an der leichten Auffindbarkeit der Adresse oder einer grundsätzlichen gesellschaftlichen Entwicklung liegt, lässt sich nicht verifizieren. Tatsache ist aber, dass parallel zum Anstieg der Social-Media-Aktivitäten des SWR auch ein rascher Anstieg von Programmbeschwerden über diesen Eingangskanal zu verzeichnen ist. Besonders das **Jugendprogramm *funk*** (https://www.funk.net/) **ist Zielscheibe von Beschwerden**. Kritikpunkt ist die nach Auffassung der meisten Beschwerdeführer einseitige politische Darstellung gesellschaftlicher Entwicklungen.
Von vielen Kanälen, die es bei ***funk*** gibt (https://www.funk.net/channel/), standen 2021 wieder das Browser Ballett (https://www.funk.net/channel/browser-ballett-800) und die Serie **Datteltäter** (https://www.funk.net/channel/datteltaeter-814) im Zentrum der Beschwerden. In der offiziellen Beschreibung von *funk* heißt es zu den Datteltätern:
„Politische Satire, deutsch-muslimisches Selbstverständnis und Vorurteile gegen Muslime in Deutschland. Einmal in der Woche räumen die Datteltäter auf YouTube mit Stereotypen auf, machen sich über Engstirnigkeit lustig und haben einfach ihren Spaß dabei. Der Fokus der Datteltäter geht dabei in eine Richtung: Gesellschaftskritik.“ Die Beschwerdeführer betrachten diese Beiträge jedoch nicht als Humor und sehen darin auch keine Satire,

sondern eine „Verhöhnung normaler deutscher Mitbürger“, zumal diese oft „als tumbe Deutsche“ dargestellt würden.

6.2 Anfragen und Auskunftsersuchen beim Beitragsservice in Köln

Beim **Zentralen Beitragsservice** in Köln werden die Auskunftsersuchen inzwischen routinemäßig bearbeitet. Die Zahl dieser **Auskunftsersuchen** ist im Vergleich zu 2020 gesunken und lag bei **6.888 im Jahr 2021**. Der Rückgang dürfte zwei Ursachen haben: Zum einen gab es 2021 keine überregionalen Aufrufe im Internet, den Beitragsservice mit Anfragen zu überschwemmen, zum anderen verlagert sich die Kritik am öffentlich-rechtlichen System vom Beitragseinzug auf die Rundfunkanstalten selbst.

Im vergangenen Jahr konnte noch festgestellt werden, dass die Zahlen beim SWR sowohl prozentual als auch absolut höher sind als bei anderen Rundfunkanstalten. Dies hat sich jetzt beruhigt. Die Anzahl der Anfragen korrelierten inzwischen mit dem Anteil der Rundfunkteilnehmer. So betreffen von den 6.888 Auskunftsersuchen **1.162** den **SWR**.

7 Organisation und Zusammenarbeit bei der Datenschutzkontrolle

7.1 Aufbau und Organisation auf europäischer Ebene

Die **EU-Datenschutz-Grundverordnung** (DSGVO) sieht die Errichtung von **Aufsichtsbehörden** vor und macht hierzu in den **Artikeln 51 ff. DSGVO** konkrete Vorgaben. Die Aufsichtsorgane müssen **unabhängig** sowie **weisungsfrei** sein und keiner Dienst-, Fach- oder Rechtsaufsicht unterliegen.

Aufgrund der durch die DSGVO geschaffenen Stellung und der dort zugewiesenen Aufgaben zur Umsetzung von grundlegendem europäischem Recht, wird man die **Aufsichtsbehörden** funktional als „**dezentrale Unionsbehörden“** bzw. „funktional teileuropäisierte Behörden“ ansehen müssen.

Die Aufsichtsbehörden müssen nicht nur untereinander zusammenarbeiten, sondern auch mit dem neu geschaffenen **Europäischen Datenschutzausschuss** (Art. 68 DSGVO), der weitreichende Aufgaben und Befugnisse hat.

7.2 Aufbau und Organisation in Deutschland

Nach der **EU-Datenschutz-Grundverordnung** (Art. 51 Abs. 1 DSGVO) 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 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 funktioniert hat.

7.3 Aufbau und Organisation bei den Rundfunkdatenschutzbeauftragten

Für die **Rundfunkanstalten** besteht aufgrund Art. 5 GG sowie Art. 85 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. DSGVO den jeweiligen Bundesländern. Sie haben für „ihre“ Rundfunkanstalten die entsprechenden Regelungen zu treffen. Dies ist inzwischen für alle Rundfunkanstalten geschehen und für den SWR aufgrund § 39 des Staatsvertrages der Länder Baden-Württemberg und Rheinland-Pfalz über den Südwestrundfunk überwiegend in **§ 27 LDSG BW** geregelt.

7.4 Zusammenarbeit aller Aufsichtsbehörden auf nationaler Ebene

Alle deutschen Datenschutz-Aufsichtsbehörden waren schon bislang zur **Zusammenarbeit verpflichtet**, die Bundesdatenschutzbeauftragte hatte bereits nach dem alten BDSG (§ 26 Abs. 4) die ausdrückliche Aufgabe, koordinierend zu wirken.

Mit der **Geltung der 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** der 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 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 DSGVO (Medien) sowie Art. 91 DSGVO (Kirchen) sind **gleichwertige Aufsichten** nach Art. 51 Abs. 2 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 nahezu 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.

Die Realität der Zusammenarbeit zwischen dem Bundes- und den Landesdatenschutzbeauftragten einerseits und den Rundfunkdatenschutzbeauftragten andererseits besteht nach wie vor in einem **bloßem Informationsaustausch** (bei dem oft auch nicht alle Landesdatenschutzbeauftragten teilnehmen). In die Informationsflüsse, insbesondere aus dem Europäischen Datenschutzausschuss (Art. 68 DSGVO), sind die öffentlich-rechtlichen Rundfunkanstalten vom Bundesdatenschutzbeauftragten nach wie vor **nicht eingebunden**.

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

Aufgrund der von den **Landesgesetzgebern** gewählten Aufsichtsstruktur sind bei den öffentlich-rechtlichen Rundfunkanstalten (mit Ausnahme von NDR und SWR) jetzt **zwei Kontrollebenen** zu unterscheiden:

7.6.1 Arbeitskreis der Datenschutzbeauftragten (AK DSB)

Alle Datenschutzbeauftragten der **öffentlich-rechtlichen Rundfunkanstalten** (ARD, ZDF, Deutsche Welle und Deutschlandradio), sowie die betriebliche Datenschutzbeauftragte des Zentralen Beitragsservice und der Datenschutzbeauftragte von arte Deutschland koordinieren ihre Datenschutzaufgaben in dem seit 1979 bestehenden **Arbeitskreis AK DSB**. Er tagt zweimal jährlich, besonders aktuelle und dringende Themen werden in Videokonferenzen 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. Seit 1.1.2019 und bis Ende 2021 lag der Vorsitz bei Herrn Dr. Heiko Neuhoff (NDR) und Herrn Stephan Schwarze (MDR) war sein Stellvertreter. Ab 2022 leiten Herr Axel Schneider (BR) und Herr Gerold Plachky (ZDF) den AKDSB.

7.6.2 Rundfunkdatenschutzkonferenz (RDSK)

Um die Zusammenarbeit im Hinblick auf die **aufsichtsrechtlichen Befugnisse,** insbesondere nach **Art. 58 DSGVO,** zu koordinieren, und weil die staatlichen Datenschützer den Rundfunkdatenschutzbeauftragten eine Mitgliedschaft in der Datenschutzkonferenz (DSK) verwehren, wurde mit der **Rundfunkdatenschutzkonferenz (RDSK)** ein eigenes Gremium geschaffen. 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 AK DSB zusammen.

Was für die Rundfunkanstalten durch § 26 Abs. 4 Medienstaatsvertrag (MStV) vorgeschrieben wird, gilt auch für die Rundfunkbeauftragten für den Datenschutz, nämlich die Verpflichtung zur Zusammenarbeit zu Erfüllung des Auftrages, der für die

Rundfunkanstalten in der Herstellung und Verbreitung von Hörfunk, Fernsehen und Internetangeboten besteht.

Die **Zusammenarbeit in der RDSK** bezieht sich u. a. auf die

- Schaffung einheitlicher Standards im Datenschutz der Rundfunkanstalten,
- eine einheitliche Auslegung datenschutzrechtlicher Vorschriften,
- die Erarbeitung von Stellungnahmen zu datenschutzpolitischen Fragen und
- die Erstellung von Orientierungshilfen, Handreichungen, Positionspapieren zu inhaltlichen, technischen oder organisatorischen Fragen des Datenschutzes.

Auf der **neuen Internetseite der RDSK** (https://www.rundfunkdatenschutzkonferenz.de/) werden jetzt deren Entschließungen, datenschutzrechtliche Eckpunkte oder Positionspapiere dargestellt (vgl. auch beispielhaft die Anlage zum TB, Ziff. 9.5: Entschließung der RDSK zur App „Clubhouse“).

Die nachfolgende Wort-/Bildmarke wurde im Mai 2021 beim Deutschen Patent- und Markenamt eingetragen:

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

8 Der Rundfunkbeauftragte für den Datenschutz im SWR

8.1 Rechtsgrundlagen

Die Aufgaben, Befugnisse und Stellung des **Rundfunkdatenschutzbeauftragten beim SWR** ergeben sich aufgrund § 39 Abs. 1 SWR-Staatsvertrag aus dem **Landesdatenschutzgesetz Baden-Württemberg** (LDSG BW) vom 12. Juni 2018 (GBl. BW, S. 173 ff.; 2018, 1549, 1551) sowie der **unmittelbar geltenden** EU-Datenschutz-Grundverordnung (**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. Dieses Gremium müsste auch für eine **amtsangemessene Einordnung in das Organisations- und Personalgefüge** des SWR (sowie eine entsprechende Besoldung; vgl. § 27 Abs. 3 Satz 2 LDSG BW) sorgen, woran es derzeit fehlt (so wurde ihm beispielsweise die Stellung als Hauptabteilungsleiter versagt). Während sowohl der Bundesdatenschutzbeauftragte als auch die Landesdatenschutzbeauftragten aufgrund der EU-Datenschutz-Grundverordnung mehr Planstellen erhielten, blieb beim SWR alles beim Alten und dies trotz der inzwischen massiven Ausweitung der datenschutzkritischen Aktivitäten in den sozialen Medien. Die linearen Programme treten gegenüber neuen **Social-Media-Anwendungen** und **Apps** zurück. Die **Hinwendung zu Facebook, Instagram oder WhatsApp** ist ungebrochen. Damit besteht aber ein erhöhter datenschutzrechtlicher Beratungsbedarf, zumal meist Programme amerikanischer Anbieter genutzt werden und Datenübermittlungen ins außereuropäische Ausland erfolgen, was nach dem EuGH Urteil vom Urteil vom 16. Juli 2020 (C-311/18) nicht nur kritisch ist, sondern zusätzliche Regelungen erfordert.

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**).

Nach § 27 Abs. 3 LDSG BW müssen dem Rundfunkbeauftragten für den Datenschutz nicht nur die „*zur Erfüllung ihrer oder seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung*“ gestellt werden, sondern notwendig ist auch: *„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.“* An allen diesen Erfordernissen fehlt es beim SWR immer noch. Die Planstelle meines Referenten taucht auch im **Haushaltsplan 2022** immer noch nicht offen auf (sondern ist irgendwo versteckt). Während der Landesgesetzgeber den Landesdatenschutzbeauftragten im neuen Haushaltsplan 2022 in einem **Einzelplan** ausgewiesen hat, fehlt es daran beim SWR. Es besteht weder ein Einzelplan, noch sind alle Planstellen *öffentlich und gesondert im Haushaltsplan* ausgewiesen.

8.3 Aufgaben und Befugnisse des Rundfunkdatenschutzbeauftragten

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

8.3.1 Aufgaben des Rundfunkdatenschutzbeauftragten

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 gesetzlichen 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).

Inzwischen explodiert der datenschutzrechtliche Beratungsbedarf im **Programmbereich** geradezu. Das lineare Angebot, also klassischer Hörfunk und Fernsehen, wird von immer mehr Social-Media-Aktivitäten überlagert. Es scheint so, als wolle der SWR jeden Hype bei **Social Media-Angeboten oder Apps** (vergleiche nur Clubhouse) mitmachen. Während bislang der SWR ein *Sender* war, der seine Angebote an ein Millionenpublikum *ausgesandt* hat, wird jetzt von einer Vielzahl differenzierter Bereiche und Redaktionen

kleinteilig mit kleinsten Gruppen in Interaktion getreten. Damit erhöht sich der Beratungsbedarf sowohl im Hinblick auf die immer neuen Ideen der Redaktionen und Nutzung datenschutzrechtlich fragwürdiger Tools, als auch den Reaktionen der angesprochenen Nutzer in den sozialen Medien bzw. und Apps, welche auf den Rundfunkbeauftragten zurückschlagen.

Im **Verwaltungsbereich** kann es nicht sein, dass der Einkauf nicht in der Lage ist, ein Vertragsmuster zur Auftragsdatenverarbeitung auszufüllen und das gigantische SAP-Projekt verschlingt eine Unmenge an Beratungszeit. Da ist es schon eine vertraute Materie, sich mit den immer kritischer und herausfordernden **Rundfunkbeitragszahlern** zu befassen.

Mit den gegenwärtigen Personalkapazitäten jedenfalls können die aktuellen und gesetzlich vorgegebenen Aufgaben nicht mehr erfüllt werden.

8.3.2 Befugnisse des Rundfunkdatenschutzbeauftragten

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 (sog. **„Mitarbeiterexzess**“).

8.4 Jährlicher Tätigkeitsbericht

Der **Tätigkeitsbericht** des Rundfunkdatenschutzbeauftragten beim SWR ist aufgrund Art. 59 DSGVO und § 27 Abs. 10 Satz 2 LDSG BW **jährlich zu erstatten**. Er wird auf **www.swr.de/datenschutz** veröffentlicht und kann als Papierdruck angefordert werden.

Abgesehen von der Veröffentlichung im Internet geht der Bericht nicht nur an die Geschäftsleitung und die Gremien des SWR, sondern muss aufgrund Art. 59 DSGVO auch

der EU-Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht werden.
§ 27 Abs. 10 Satz 2 LDSG BW bestimmt darüber hinaus: „*Der Bericht wird den **Landtagen** und den **Landesregierungen** der unterzeichnenden Länder des Staatsvertrages über den Südwestrundfunk **übermittelt**.“*

8.5 Tatkräftige Unterstützung und Dank

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

Meine langjährige **Amtszeit** als Rundfunkbeauftragter für den Datenschutz **endet**. Deshalb möchte ich mich auch bei **denjenigen** vielen **Mitarbeiterinnen und Mitarbeiter** im SWR (sowie vormals im SDR) bedanken, die bereit waren, mich bei meiner Aufgabe zu unterstützen.

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
www.swr.de/datenschutz

9 Anhang

Übersicht:

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 Dienstort 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 Gesetze zur Datenverarbeitung zu journalistischen Zwecken in Hörfunk und Fernsehen sowie bei Telemedien

Für die **Datenverarbeitung zu journalistischen Zwecken** gelten als Folge des Gebotes in Art. 85 DSGVO Sonderregelungen („Medienprivileg“). Diese waren bis zum 6. November 2020 in § 9c und § 57 des als Landesgesetz erlassenen Rundfunkstaatsvertrag (RStV**)** geregelt gewesen (GBl. BW 2018, S. 129 ff.). **Jetzt** und damit auch im Berichtszeitraum 2021 sind diese Regelungen gleichlautend **im Medienstaatsvertrag enthalten** (MStV) zwar in den **§§ 12 und 23 MStV**. Der Medienstaatsvertrag (MStV) vom 15. April 2020 wurde verkündet als Artikel 1 des Staatsvertrags zur Modernisierung der Medienordnung in Deutschland (GBl. BW 2020, S. 429, 430; 1063; GVBl. RP 2020, 377; 674).

§ 12 MStV
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) 2016/679 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; L 127 vom 23. Mai 2018, S. 2) 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 Person 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 dieses Staatsvertrages bleiben unberührt.

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

§ 23 MStV
Datenverarbeitung zu journalistischen Zwecken, Medienprivileg

(1) Soweit die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio, private Rundfunkveranstalter oder Unternehmen und Hilfsunternehmen der Presse als Anbieter von Telemedien 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 außer den Kapiteln I, VIII, X und XI der Verordnung (EU) 2016/679 nur die Artikel 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Artikel 24 und Artikel 32 der Verordnung (EU) 2016/679 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. Kapitel VIII der Verordnung (EU) 2016/679 findet keine Anwendung, soweit Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserates unterliegen. Die Sätze 1 bis 6 gelten entsprechend für die zu den in Satz 1 genannten Stellen gehörenden Hilfs- und Beteiligungsunternehmen. Den betroffenen Personen stehen nur die in den Absätzen 2 und 3 genannten Rechte zu.

(2) Werden personenbezogene Daten von einem Anbieter von Telemedien zu journalistischen Zwecken gespeichert, verändert, übermittelt, gesperrt oder gelöscht und wird die betroffene Person dadurch in ihrem Persönlichkeitsrecht beeinträchtigt, kann sie Auskunft über die 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 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 des Anbieters 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. Die Sätze 1 bis 3 gelten nicht für Angebote von Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse, soweit diese der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserates unterliegen.

(3) Führt die journalistische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, 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.

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 2018, 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 Rundfunkbeauftrage für den Datenschutz oder den Rundfunk-beauftragten 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 im Jahre 2021

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	Ivka Jurčević 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 Entschließung der Rundfunkdatenschutzkonferenz (RDSK):

RDSK
RUNDFUNKDATENSCHUTZKONFERENZ

Entschließung der RDSK

Auch abrufbar unter https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen
Vgl. auch Ziff. 2.1 meines 13. TB (2020), S. 15

Entschließung der RDSK zu „Clubhouse“

Clubhouse ist eine neue App für Audio-Talkshows. Über sie kann sich der App-Nutzer **Gespräche anhören und an Diskussionen teilnehmen**. Es sind öffentliche Diskussionen (vergleichbar virtuell gestalteten Podiumsdiskussionen), aber auch geschlossene Gruppen möglich. Ein Moderator spricht live über ein bestimmtes Thema und der Nutzer kann als Zuhörer teilnehmen. Er ist zunächst stumm geschaltet, kann aber vom Moderator zum Gespräch freigeschaltet werden. **Clubhouse ist** also eine **Art „Live-Talkshow“ ohne Kamera** (und Textnachrichten).

Datenschutzrechtlich ist diese neue App aus mehreren **Gründen** sehr **bedenklich**:

- **Zugriff auf Kontakte**
  Die App erfordert den Zugriff auf alle auf dem Gerät des Nutzers gespeicherten Kontakte, wenn dieser selbst zu einer Gesprächsrunde einladen will. Er muss also die **Kontaktdaten Dritter** (die neben den Telefonnummern auch E-Mail-Adressen und Wohnadressen sein können) auf dem Smartphone mit Clubhouse teilen. Damit erhält Clubhouse zum einen Informationen über das **soziale Umfeld** des Nutzers. Zum anderen werden die Kontaktdaten von Personen, die noch nicht bei Clubhouse registriert sind, ohne deren Einwilligung an das Unternehmen übermittelt. Bei der Anmeldung über einen Social-Media-Account behält sich Clubhouse den Zugang für Follower und Freundeslisten vor.

- **Audiomitschnitte und Speicherung in den USA**
  Clubhouse fertigt Audiomitschnitte, die nach eigenen Angaben ausschließlich zur Unterstützung der Untersuchung von Vorfällen aufgezeichnet werden. Diese werden ebenso wie die erhobenen Kontakt- und Accountinformationen der Nutzer und Dritter zumindest für gewisse Zeit **in den USA gespeichert** und verarbeitet sowie an verschiedene Unternehmen weitergegeben. Zusagen über ein der DSGVO vergleichbares angemessenes Niveau zum Schutz dieser Daten enthält die Datenschutzerklärung des Anbieters bislang nicht. Ohne entsprechende Vorkehrungen verstößt die Datenübermittlung in die USA gegen die DSGVO (vgl. das EuGH-Urteil vom 16.7.2020, C-311/18 zum Privacy Shield).

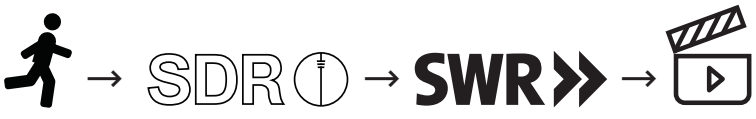
- **Fehlende Transparenz**
  In den Allgemeinen Geschäftsbedingungen („Terms of Service“) und der unzulässigerweise nur in englischer Sprache formulierten Datenschutzerklärung („Privacy Policy“) von Clubhouse wird die DSGVO bislang nicht erwähnt und eine Adresse für Datenschutzauskünfte in der EU bzw. ein Vertreter nach Art. 17 DSGVO nicht benannt. Ein **Tracking** kann wohl nicht verhindert werden und eine **Profilbildung des Nutzers** ist möglich. Wer zu den Empfängern der personenbezogenen Daten gehört und ob und in welchem Umfang Daten an Geschäftspartner verkauft werden, ist unklar und wird nicht transparent kommuniziert.

Zusammenfassend lässt sich feststellen: Von der **Nutzung dieser App ist bis auf weiteres dringend abzuraten**. Die RDSK fordert die Rundfunkanstalten und ihre Beteiligungsunternehmen auf, die Installation der App auf allen dienstlich zur Verfügung gestellten Geräten, mindestens aber einen Zugriff der App auf das dienstliche Kontaktverzeichnis wirksam und vollständig zu unterbinden, bis der Anbieter eine DSGVO-konforme Nutzung ermöglicht hat.
Februar 2021

10 Stichwortverzeichnis

Südwestrundfunk
Neckarstraße 230
70190 Stuttgart

SWR.de/Datenschutz



Klappe zu – letzter Tätigkeitsbericht
von Prof. Dr. Armin Herb.