DATENSCHUTZ TROTZT LOCKDOWN

13. TÄTIGKEITSBERICHT DES DATENSCHUTZBEAUFTRAGTEN

1. Januar – 31. Dezember 2020 • Prof. Dr. Armin Herb

13. Tätigkeitsbericht

des Rundfunkbeauftragten für den Datenschutz des Südwestrundfunks

Prof. Dr. Armin Herb

Berichtszeitraum: 1.1.2020 bis 31.12.2020

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 2019, 1549, 1551) dem Rundfunkrat, dem Verwaltungsrat, dem Intendanten des SWR sowie den Landtagen und Landesregierungen Baden-Württemberg und Rheinland-Pfalz.

INHALTSVERZEICHNIS

ZUSAMMENFASSENDE WÜRDIGUNG 5

1 ENTWICKLUNG DES DATENSCHUTZRECHTS IM JAHR 2020 7

1.1 Europäische Datenschutz-Grundverordnung 7

1.2 Weitere europäische Verordnungen und Richtlinien zum Datenschutz 8

1.2.1 ePrivacy-VO als Nachfolge der RiLi 2002/58 zur elektronischen Kommunikation 8

1.2.2 EU-Richtlinie zum Schutz von Personen, die Verstöße melden ("Whistleblower-RiLi") 8

1.2.3 Richtlinienentwurf vom 16.12.2020 zur Cybersicherheit und Verschlüsselung 9

1.2.4 Gesetzespaket für digitale Dienste („Digital Services Act Package") 9

1.3 Gesetzgebung im Bereich des Bundes 10

1.3.1 Gesetz zur Verbesserung des Persönlichkeitsschutzes bei Bildaufnahmen 10

1.3.2 Gesetz zur Einführung und Verwendung einer Identifikationsnummer 10

1.3.3 Gesetzentwurf zur Überwachung durch den BND 11

1.3.4 Gesetzentwurf zur Telekommunikationsmodernisierung 12

1.3.5 Entwurf „Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)" 12

1.3.6 Entwurf eines IT-Sicherheitsgesetzes 2.0 12

1.4 Gesetzgebung im Bereich der Zuständigkeit der Länder 13

1.4.1 Medienstaatsvertrag (MStV) 13

1.4.2 Erster Medienänderungs-Staatsvertrag 14

1.5 Datenschutzrichtlinie des Europarates („Konvention 108") 14

2 DATENSCHUTZ IM PROGRAMM- UND PRODUKTIONSBEREICH DES SWR 15

2.1 Der große Hype: Clubhouse, eine neue App für Hörfunk-Talkshows 15

2.2 Abnahmetool für Videomaterial 16

2.3 Auf digitaler Spurensuche – Tracking 17

2.4 Dauerbelastung: Auftragsverarbeitungsverträge ohne Ende 18

2.5 ARD-Hörspieltage in Pandemiezeiten 19

2.6 Transparenz durch Datenschutzerklärungen 20

2.7 Google Firebase in der ARD-Mediathek 21

2.8 Wahl des Orchestervorstands des SWR Symphonieorchesters 22

2.9 SWR Symphonieorchester, Corona und die Wissenschaft 22

2.10 WhatsApp minimieren! ... 23
2.11 ARD Retro – Archivmaterial und Datenschutz ... 24
2.12 Augen auf bei der Partnerwahl ... 24

3 DATENSCHUTZ IM VERWALTUNGSBEREICH DES SWR ... 26

3.1 SAP-Prozessharmonisierung ... 26
3.1.1 Grafik SAP Gesamtprojekt-Leitdokumentation ... 27
3.1.2 SAP-Solution Manager ... 27
3.2 Neue Kameras im Eingangsbereich und Foyer ... 29
3.3 Parkberechtigung mit QR-Code in Baden-Baden ... 29
3.4 Selbstaufschreibung im Projekt PS² ... 30
3.5 Kabelhilfen ohne WhatsApp-Anschluss ... 30
3.6 Unendlich unverständlich ... 31
3.7 Microsoft Office 365 ... 31
3.7.1 Microsoft Forms ... 32
3.7.2 Microsoft Sway ... 32
3.7.3 Microsoft Teams ... 33

4 DATENSCHUTZ BEIM ARD ZDF DEUTSCHLANDRADIO BEITRAGSSERVICE ... 35

4.1 Grundlagen zum Rundfunkbeitrag ... 35
4.2 Datenbestand beim Zentralen Beitragsservice und beim SWR ... 36
4.3 Meldedatenabgleich ... 36
4.4 Tücken der Telearbeit und Pannen im Home Office durch die Corona-Pandemie ... 37
4.5 Vereinbarung zur gemeinsamen Verantwortlichkeit („Joint-Controllers“) ... 38
4.6 Neuer Inkasso-Dienstleister ... 38
4.7 Kundenkontakt-Management ... 38
4.8 EUDAGO ... 39

5 DATENSICHERHEIT IM SWR ... 41

5.1 Multi-Faktor-Authentifizierung (MFA) für Office 365 bzw. Microsoft 365 ... 41
5.2 Datensicherheit im Home Office, nicht nur in Corona Zeiten ... 41
5.3 SWR-IT-Sicherheitskonferenz ... 42
5.4 Penetrationstest ... 43
5.5 Datenerhebung ohne Rechtsgrundlage durch die KEF ... 43

6. AUSKUNFTSERSUCHEN UND BESCHWERDEN 44

6.1 BEIM SWR EINGEGANGENE AUSKUNFTSERSUCHEN UND BESCHWERDEN 44

6.1.1 Direkteingaben zum Rundfunkbeitragseinzug 45

6.1.2 Sonstige Direkteingaben beim Rundfunkdatenschutzbeauftragten 45

6.2 ANFRAGEN UND AUSKUNFTSERSUCHEN BEIM BEITRAGSSERVICE IN KÖLN 46

7 ORGANISATION UND ZUSAMMENARBEIT BEI DER DATENSCHUTZKONTROLLE 48

7.1 AUFBAU UND ORGANISATION AUF EUROPÄISCHER EBENE 48

7.2 AUFBAU UND ORGANISATION IN DEUTSCHLAND 48

7.3 AUFBAU UND ORGANISATION BEI DEN RUNDFUNKDATENSCHUTZBEAUFTRAGTEN 49

7.4 ZUSAMMENARBEIT ALLER AUFSICHTSBEHÖRDEN AUF NATIONALER EBENE 49

7.5 ZUSAMMENARBEIT DER DATENSCHUTZBEAUFTRAGTEN AUF LÄNDEREBENE 51

7.6 KONFERENZ UND ARBEITSKREIS DER RUNDFUNKDATENSCHUTZBEAUFTRAGTEN 51

7.6.1 Arbeitskreis der Datenschutzbeauftragten (AK DSB) 51

7.6.2 Rundfunkdatenschutzkonferenz (RDSK) 52

8 DER RUNDFUNKBEAUFTRAGTE FÜR DEN DATENSCHUTZ IM SWR 53

8.1 RECHTSGRUNDLAGEN 53

8.2 STELLUNG DES RUNDFUNKDATENSCHUTZBEAUFTRAGTEN 53

8.3 AUFGABEN UND BEFUGNISSE DES RUNDFUNKDATENSCHUTZBEAUFTRAGTEN 53

8.3.1 Aufgaben des Rundfunkdatenschutzbeauftragten 54

8.3.2 Befugnisse des Rundfunkdatenschutzbeauftragten 54

8.4 JÄHRLICHER TÄTIGKEITSBERICHT 55

8.5 TATKRÄFTIGE UNTERSTÜTZUNG 55

9 ANHANG 56

9.1 § 39 STAATSVERTRAG ÜBER DEN SÜDWESTRUNDFUNK 56

9.2 GESETZE ZUR DATENVERARBEITUNG ZU JOURNALISTISCHEN ZWECKEN IN HÖRFUNK UND FERNSEHEN SOWIE BEI TELEMEDIEN 56

9.3 § 27 LANDESDATENSCHUTZGESETZ BADEN-WÜRTTEMBERG (LDSG BW) 59

9.4 LISTE DER AUFSICHTSBEHÖRDEN NACH ARTIKEL 51 FF. DSGVO ÜBER ARD, ZDF, DW, DLR 62

9.5 EMPFEHLUNGEN DER RUNDFUNKDATENSCHUTZKONFERENZ (RDSK): 63

10 STICHWORTVERZEICHNIS 66

Zusammenfassende Würdigung

Mitten in der **Umsetzung der EU-Datenschutzverordnung** (DSGVO) vom Mai 2018 wurde die Welt von einer Pandemie erfasst. Videokonferenzen und Home Office prägten die Arbeitswelt und das Leben zu Hause.

Auch 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 2020 stellt wieder **im ersten Abschnitt** die unverminderten und immer **komplexer werdenden gesetzgeberischen Aktivitäten** dar. Herausragendes Ereignis war 2022 der neue Mediendienste-Staatsvertrag (MStV). Die **Auslegung** der Datenschutzgesetze wird von seitenlangen Ausführungen des Europäischen Gerichtshofes (**EuGH**) **und** des **Europäischen Datenschutzausschusses** geprägt.

Datenschutzfragen nehmen nicht nur pandemiebedingt insbesondere **im Programmbereich** des SWR zu (**zweiter Abschnitt**). Die **Ausweitung** der SWR-Aktivitäten **im Onlinebereich** erhöhen den datenschutzrechtlichen Beratungsbedarf enorm. Die linearen Programme treten gegenüber neuen **Social-Media-Anwendungen** und **Apps** zurück. Man scheint jeden neuen Hype wie *Clubhouse*, eine App für Hörfunk-Talkshows mitmachen zu wollen (Ziff. 2.1). Die **Hinwendung zu Facebook, Instagram oder WhatsApp** (Ziff. 2.10) ist ungebrochen. Immer neue Werkzeuge („Tools“) zur Reichweitenmessung („Tracking“) erfordern Auftragsdatenverarbeitungsverträge, die über das Datenschutzdezernat, statt den Fachabteilungen laufen (Ziff. 2.3 und 2.4). Es bedarf besonderer Anstrengungen, die Persönlichkeitsrechte der Zuhörer, Zuschauer und Internetnutzer, die immer kritischer werden, zu gewährleisten.

Einsparungen, Umstrukturierung und **Home Office** durch das Coronavirus lassen den Datenschutz **im Verwaltungsbereich** (**dritter Abschnitt**) nicht zur Ruhe kommen. Das riesige **Mammutprojekt SAP** fordert die Datenschutzbeauftragten aufs Äußerste (Ziff. 3.1). Leider sind immer noch nicht alle Mitarbeiter auf die Vertraulichkeit verpflichtet (vgl. Ziff. 3.6).

Beim **Klassiker**, dem Datenschutz beim **Beitragsservice** sind die DSGVO-Anforderungen mit immer mehr Aufwand verbunden (**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 der **Datenschutzkontrolle** bei den **öffentlich-rechtlichen Rundfunkanstalten** war im Jahr 2020 weitgehend abgeschlossen. Doch die jetzt außerhalb des SWR bestehenden **Strukturen erhöhen den Arbeitsaufwand** (Ziff. 7.6). Nach wie vor besteht bei der Zusammenarbeit mit den **staatlichen Datenschutzbeauftragten** des Bundes und der Länder (Ziff. 7.4) noch sehr viel Luft nach oben (**siebter Abschnitt**).

Abgerundet wird der Bericht durch Darstellung des Rundfunkbeauftragten für den Datenschutz im SWR, dessen gesetzlich vorgegebene **Aufgabenerfüllung** weitere Ressourcen benötigt (Ziff. 8.3 im **achten Abschnitt)**.

Stuttgart im Januar 2021 Prof. Dr. Armin Herb

1 Entwicklung des Datenschutzrechts im Jahr 2020

Die Auslegung der **EU-Datenschutz-Grundverordnung** (DSGVO) vom 25. Mai 2018 beschäftigt nach wie vor Rechtsprechung und Praxis. Die Einzelheiten der **Umsetzung sind bis heute offen und umstritten**. In vielen Bereichen gibt es weder eine einheitliche Rechtsauffassung der Aufsichtsbehörden noch eine gesicherte Rechtsprechung. Stellvertretend und spektakulär kann das **Urteil des Europäischen Gerichtshofes vom 16. Juli 2020 zum sogenannten Privacy Shield Abkommen** herangezogen werden. Der EuGH stellt die Unwirksamkeit fest und in der Praxis gibt es keine Lösungen. Das Gegenteil ist der Fall: Manche Aufsichtsbehörden drohen sogar den Unternehmen mit Bußgeld, wenn sie immer noch eine entsprechende Datenübermittlung ins außereuropäische Ausland vornehmen. 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. Im Jahr 2020 stechen zwei Entscheidungen heraus: In seinem Urteil vom 16. Juli 2020 (C-311/18) hat der EuGH den Beschluss 2016/1250 der Europäischen Kommission zur **Übermittlung personenbezogener Daten in die USA** (**Privacy Shield**; auch Schrems II genannt) für unwirksam erklärt. Eine Datenübermittlung in die USA, wo die meisten der Softwareunternehmen sitzen, ist zukünftig höchstens dann zulässig, wenn die **Standardvertragsklauseln** der EU-Kommission verwendet werden **und zusätzliche Garantien** vereinbart werden. In Betracht kommt eine Ende-zu-Ende Verschlüsselung, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann.

Möglich bleibt auch eine Anonymisierung oder Pseudonymisierung, bei der nur der Datenexporteur die Zuordnung vornehmen kann. In vier Urteilen vom 6.10.2020 hat der EuGH seine Auffassung zur **Vorratsdatenspeicherung** fortgeschrieben, konkretisiert und zum Teil neu ausgerichtet.

1.2 Weitere europäische Verordnungen und Richtlinien zum Datenschutz

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

Gleichzeitig mit der EU-Datenschutz-Grundverordnung sollte auch eine sogenannte **ePrivacy-Verordnung** veröffentlicht werden. Darauf warten die Rechtsanwender bis heute, was misslich ist, weil damit nach wie vor **keine Rechtsklarheit** im Hinblick auf **Trackingverfahren und Cookies** besteht (vgl. bereits Ziff. 1.2.2 des 10. Tätigkeitsberichts).

1.2.2 EU-Richtlinie zum Schutz von Personen, die Verstöße melden ("Whistleblower-RiLi")

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

Die Vorschrift bezweckt den **Schutz von Hinweisgebern** (Whistleblower bzw. Informanten). Dazu werden die Mitgliedstaaten verpflichtet, entsprechende gesetzliche Bestimmungen zu schaffen. Die Richtlinie fordert zunächst Regelungen bei **Verstößen gegen das Unionsrecht** (Art. 1). Dazu wird in einer umfangreichen Anlage aufgeschlüsselt, welche Richtlinien und Verordnungen der EU darunterfallen. Wie sich aus dem Erwägungsgrund 14 ergibt, wird die Meldung von Hinweisgebern als besonders nützlich angesehen, wenn dadurch Sicherheitsvorfälle oder **Verstöße gegen die Datenschutzvorschriften der EU** verhindert werden. Deshalb sollen beispielsweise auch Hinweise von Informanten im Hinblick auf die Datenschutz-Grundverordnung, sowie die

Richtlinie für die elektronische Kommunikation oder diejenige zur Gewährleistung der Netz- und Informationssicherheit in der EU durch die Vorschrift geschützt werden (vergleiche in der RiLi Ziff. J des Anhangs, Teil I – L 305/55). Die Richtlinie lässt aber die Befugnis der Mitgliedstaaten unberührt, den Schutz auf andere Bereiche der Rechtsakte auszudehnen (Art. 2 Abs. 2).

Auch der SWR wird betroffen sein, da die Richtlinie Behörden und öffentliche Stellen **erfasst**. Es müssen deshalb **im SWR zukünftig entsprechende Hinweisgebersysteme etabliert** werden. Bislang ist offen, wann der Bund ein entsprechendes Gesetz verabschiedet, da Mitte Dezember 2020 noch keine Einigkeit in der Regierungskoalition bestanden hat.

1.2.3 Richtlinienentwurf vom 16.12.2020 zur Cybersicherheit und Verschlüsselung

Ende des Jahres 2020 hat der EU-Ministerrat eine unverbindliche Resolution verabschiedet, in der faktisch die **Abschaffung der Ende-zu-Ende-Verschlüsselung** in der EU gefordert wurde. Auch massive Proteste konnten nicht verhindern, dass am 16.12.2020 der **Entwurf einer Richtlinie** "zu Maßnahmen für hochklassige Cybersicherheit" vorgelegt wurde. Danach soll auch die Möglichkeit des Zugriffs auf den **verschlüsselten Datenverkehr** möglich sein, womit es dann faktisch **keinen Informantenschutz beim elektronischen Datenaustausch mehr** geben kann. Die weiteren Beratungen werden zeigen, wie es hier weitergeht.

1.2.4 Gesetzespaket für digitale Dienste („Digital Services Act Package“)

Die **EU-Kommission** hat am 27. Mai 2020 ihr Arbeitsprogramm vorgelegt. Danach soll auch ein Gesetzespaket für digitale Dienste geschaffen werden, das sog. „**Digital Services Act Package**“, das sich in zwei Bereiche unterteilt:

- 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.

Deshalb hat die Europäische Kommission am 15. Dezember 2020 mit Vorschlägen für einen Digital Services Act (DSA) und einen Digital Markets Act (DMA) einen Rechtsetzungsprozess gestartet, in dessen Ergebnis der digitale Raum in der Gesellschaft rechtlich neu vermessen und organisiert würde. Dies wirft auch Fragen zur **Kompetenzverteilung** zwischen der Europäischen Union und den Mitgliedstaaten **im Mediensektor** auf.

1.3 Gesetzgebung im Bereich des Bundes

Der Bundesgesetzgeber hat im Jahr 2020 eine Vielzahl von Gesetzen mit Bezug zum Datenschutzrecht erlassen oder kurz vor Jahresende entsprechende Kabinettsbeschlüsse gefasst, die sich durch eine selbst vom Bundesrat beklagte, unverhältnismäßig kurze Frist zur Stellungnahme auszeichneten. Die Gesetzesvorhaben wurden insbesondere in der Sitzung des Bundeskabinetts am 16.12.2020 verabschiedet und sollen alle bis zur Sommerpause durchgezogen werden, weil danach die Bundestagswahl stattfindet.

1.3.1 Gesetz zur Verbesserung des Persönlichkeitsschutzes bei Bildaufnahmen

Durch die Änderungen im Strafgesetzbuch wird der Persönlichkeitsschutz bei Bildaufnahmen gestärkt. Zukünftig kann die „**Verletzung des Intimbereichs durch Bildaufnahmen**“ mit dem **neuen § 184 k StGB bestraft werden** und **§ 201 a StGB** („Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen“) wird **auf verstorbene Personen ausgedehnt**. In beiden Fällen bleibt wie bislang eine berechtigte Berichterstattung davon unberührt.

1.3.2 Gesetz zur Einführung und Verwendung einer Identifikationsnummer

Am 28.1.2021 hat der Bundestag das sog. „**Registermodernisierungsgesetz**“ (RegMoG) verabschiedet (vgl. BTagsDrs. 19/24226 sowie 19/ 26247). Damit 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. Noch bei der damaligen Verabschiedung zur Änderung der Abgabenordnung (vgl. § 139a AO) hatte der damalige Finanzminister Peer Steinbrück 2007 erklärt, das steuerliche Identifikationsmerkmal diene allein **steuerlichen** Zwecken. Dies ist jedoch mit dem jetzigen Registermodernisierungsgesetz nicht mehr der Fall. Die **Steueridentifikationsnummer** wird 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. Nicht nur der Bundesdatenschutzbeauftragte lehnte den Gesetzesentwurf als „**vollständige Registrierung und Katalogisierung der Persönlichkeit**“ ab, sondern auch aus dem Bundesrat kam Kritik, wie in der öffentlichen Anhörung im Innenausschuss am 14.12.2020 zum Gesetzentwurf deutlich wurde. Trotzdem hat der Bundestag am 28.1.2021 das Gesetz beschlossen und wahrscheinlich wird sich das **Bundesverfassungsgericht** damit beschäftigen müssen, ob die **Steuer-ID als Personenkennzeichen** verwendet werden darf.

1.3.3 Gesetzentwurf zur Überwachung durch den BND

In dem Urteil vom 19. Mai 2020 (1 BvR 2835/17) zur Fernmeldeaufklärung nach dem BND-Gesetz (Telekommunikationsüberwachung) hat das Bundesverfassungsgericht festgestellt, dass "besondere Anforderungen an den **Schutz von Vertraulichkeitsbeziehungen**, wie insbesondere **zwischen Journalisten und ihren Informanten** oder Rechtsanwälten und ihren Mandanten", zu stellen sind (Rn. 193 des Urteils). Gegenüber diesen Personengruppen müsste die gezielte Überwachung begrenzt werden (Rn. 194). Zwar seien Überwachungsmaßnahmen auch hier nicht ausgeschlossen, doch müssten diese besonders ausgestaltet werden (Rn. 257, 258).

Im **Gesetzentwurf** vom 25.1.2020 (BTagsDrs. 19/26103) ist vorgesehen, das Gesetz über den Bundesnachrichtendienst (BND-Gesetz), das Artikel-10-Gesetz, die Telekommunikations-Überwachungsverordnung sowie weitere Gesetze zu ändern. Dort sind im Grundsatz auch Normen zum „**Schutz von Vertraulichkeitsbeziehungen“**

vorgesehen. Inwieweit hier tatsächlich auf die besonderen **Belange von Journalisten** und Rechtsanwälten Rücksicht genommen wird, dürfte sich erst im Gesetzgebungsverfahren im Laufe des Jahres 2021 zeigen.

1.3.4 Gesetzentwurf zur Telekommunikationsmodernisierung

Ein weiterer Gesetzentwurf wurde am 16.12.2020 im Bundeskabinett behandelt, und zwar zur **Modernisierung des Telekommunikationsrechts**. Damit soll insbesondere die EU-Richtlinie 2018/1972 über den europäischen Kodex für die elektronische Kommunikation umgesetzt werden.

1.3.5 Entwurf „Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)“

Schließlich ist seit einiger Zeit auch ein sog. **„Telekommunikations-Telemedien-Datenschutz-Gesetz“ (TTDSG)** auf dem Markt. Ziel des Entwurfes ist es, ein abgeschlossenes Spezialgesetz zum Datenschutz und zum Schutz der Privatsphäre im Bereich der Telekommunikation und der Telemedien (also z. B. Apps und Webseiten) zu schaffen, denn – so die Begründung – das **Nebeneinander von DSGVO, TMG und TKG** führe zu Rechtsunsicherheiten bei denjenigen, die Telemedien und Telekommunikationsdienste nutzten. Im Entwurf werden Vorgaben für Cookies gemacht (welche mit einer ePrivacy-VO der EU – siehe oben Ziff. 1.2.1 - in Einklang stehen müssten), Einwilligungsregelungen eingeführt und für bestimmte Telemedien-Anbieter sogar eine Registrierungspflicht vorgesehen.

1.3.6 Entwurf eines IT-Sicherheitsgesetzes 2.0

Als weiterer Gesetzentwurf wurde ein „**Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“** (IT-Sicherheitsgesetz 2.0) im Januar in den Bundestag eingebracht (BTags-Drs. 19/26106 vom 25.1.021). Danach sollen nicht nur sog. „kritische Unternehmen“, sondern auch solche von „besonderem öffentlichen Interesse“ einbezogen werden, dem Bundesamt für Informationssicherheit (BSI) Maßnahmen zur **Detektion von Sicherheitslücken** erlaubt werden („staatliches Hacking“) und die Verpflichtung bestehen, der Behörde **Sicherheitskonzepte vorzulegen** und zudem kann diese den **Einsatz kritischer Komponenten untersagen**. Hier wird

darauf zu achten sein, dass nicht die Unabhängigkeit der öffentlich-rechtlichen Rundfunkanstalten über die Hintertür der IT-Sicherheit durch staatliche Eingriffe gefährdet wird.

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.

Ein **Meilenstein** im Jahr 2020 war dabei der **Medienstaatsvertrag (MStV)**, welcher den Rundfunkstaatsvertrag (RStV) der Länder ablöst. Er wurde in Baden-Württemberg und Rheinland-Pfalz als Artikel 1 des Staatsvertrags zur Modernisierung der Medienordnung in Deutschland als Landesgesetz erlassen (GBl. BW 2020, S. 429, 430; 1063; GVBl. RP 2020, 377; 674).

1.4.1 Medienstaatsvertrag (MStV)

Zwischen dem 14. und dem 28. April 2020 haben die Ministerpräsidenten den Staatsvertrag zur **Modernisierung der Medienordnung in Deutschland** unterschrieben. Er soll die Grundlage für eine aktuelle Medienregulierung sein und die tiefgreifenden Veränderungen im Medienbereich erfassen, die insbesondere durch die Digitalisierung, geändertes Nutzungsverhalten und die zunehmende Bedeutung von Plattformen, Benutzeroberflächen und Intermediären ausgelöst wurde. Der **Medienstaatsvertrag (MStV)** ersetzt nicht nur den bisher am Rundfunkbegriff orientierten Rundfunkstaatsvertrag (RStV), sondern will eine umfassende Regulierung (auch beim Jugendschutz) und eine **zeitgemäße Medienordnung** schaffen. Nachdem er von allen Ländern ratifiziert worden ist, konnte er in den Gesetzblättern der Länder veröffentlicht werden (z. B. GBl. BW 2020, Seiten 429 ff. und GVBl. RP 2020, Seiten 377 ff.). Die **Datenverarbeitung zu journalistischen Zwecken** bzw. das Medienprivileg werden in Konkretisierung von Art. 85 DSGVO in den §§ 12 und 23 MStV geregelt (vgl. die Anlage zum TB sowie zum „Mediendatenschutz zwischen neuem Medienstaatsvertrag und der EU-Datenschutz-Grundverordnung (DSGVO), insbesondere am Beispiel des SWR“, auch

den Aufsatz in den Verwaltungsblättern Baden-Württemberg, Dezember-Heft 2020, Seite 492 ff.).

1.4.2 Erster Medienänderungs-Staatsvertrag

Die Ministerpräsidenten der Länder haben im Rahmen des 1. Medienänderungs-Staatsvertrages die **Erhöhung des Rundfunkbeitrages zum 1.1.2021** vorgesehen. Nachdem aber aufgrund des Verhaltens des Landes **Sachsen-Anhalt** nicht alle Ratifizierungsurkunden bis Ende 2020 hinterlegt werden konnten, trat dieser Staatsvertrag nicht in Kraft. Die öffentlich-rechtlichen Rundfunkanstalten haben deshalb **Klage vor dem Bundesverfassungsgericht** erhoben.

1.5 Datenschutzrichtlinie des Europarates („Konvention 108“)

Der **Europarat** hat bereits 1981 das internationale „**Übereinkommen zum Schutz des Menschen** bei der automatischen Verarbeitung personenbezogener Daten“ (gemeinhin als „Konvention 108“ bezeichnet) verabschiedet (BGBl. 1985 II, S. 538 f.). Nach mehrjährigen Verhandlungen erfolgte eine **Modernisierung** (welche auch die DSGVO berücksichtigt), wodurch beispielsweise Betroffenenrechte gestärkt, Meldepflichten bei Datenschutzverletzungen eingeführt und die Schaffung einer unabhängigen Aufsichtsbehörde für alle Konventionsstaaten verpflichtend gemacht wird. Jetzt hat auch Deutschland das **Abkommen ratifiziert und im Gesetzblatt veröffentlicht** (BGBl. 2020 II, S. 874 f.).

2 Datenschutz im Programm- und Produktionsbereich des SWR

2.1 Der große Hype: Clubhouse, eine neue App für Hörfunk-Talkshows

Bei **Clubhouse** kann sich der App-Nutzer **Gespräche anhören und an Diskussionen teilnehmen**. Es sind öffentliche Diskussionen (vergleichbar virtuell gestalteten Podiumsdiskussionen), aber auch geschlossene Gruppen sind 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 aufgrund mehrerer **Gründe** sehr **bedenklich**.

- **Zugriff auf Kontakte**
  Schon die Registrierung erfordert den Zugriff auf alle Kontakte im Adressbuch des Nutzers. Es müssen also die **eigenen Kontakte** (die neben den Telefonnummern auch E-Mail-Adressen und Wohnadressen sein können) auf dem Smartphone mit Clubhouse geteilt werden. Damit kann Clubhouse zum einen das **soziale Umfeld** des Nutzers ausspionieren. Zum anderen werden die Kontaktdaten von Personen, die noch nicht bei Clubhouse registriert sind, ohne deren Einwilligung an das Unternehmen übermittelt. Das gesamte **Netzwerk einer Person** ist für alle Nutzer weitgehend einsehbar. Über den Klartextnamen können so Äußerungen schnell einer Person zugeordnet werden kann. Bei der Anmeldung über einen Social-Media-Account behält sich Clubhouse den Zugang für Follower und Freundeslisten vor.
- **Audiomitschnitte und Speicherung in den USA**
  Es werden Audiomitschnitte gefertigt, die nach Angaben von Clubhouse ausschließlich zur Unterstützung der Untersuchung von Vorfällen aufgezeichnet werden. Diese werden ebenso wie die erhobenen Kontakt- und Accountinformationen der Nutzer und Dritter **in den USA gespeichert** und verarbeitet. Damit besteht auch hier das Problem der Datenübermittlung ins Ausland (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 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 existieren nicht. 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.
- **Kritische AGBs**
  In den Allgemeinen Geschäftsbedingungen wird die geschäftliche Nutzung verboten und der Verbraucherzentrale Bundesverband (vzbv) hat Clubhouse bereits abgemahnt, weil die **AGBs nicht in Deutsch** sind und **kein Impressum** vorhanden ist.

Zusammenfassend lässt sich feststellen: Auch wenn sich auf Clubhouse wohl ein Ministerpräsident tummelt, ist von der **Nutzung dieser App dringend abzuraten**.

2.2 Abnahmetool für Videomaterial

Einsparungen führen auch im Programm dazu, dass immer mehr Aufgaben von Drittfirmen erledigt werden. So beauftragt der SWR vermehrt externe Produktionsfirmen mit der Erstellung von **sendefähigem Videomaterial für Drittplattformen**, wie z. B. YouTube. Bevor das Videomaterial auf Sendung gehen kann, bedarf es einer Abnahme, um den hohen Qualitätsstandards des SWR zu genügen. Diese Abnahmen gestalten sich in der Regel arbeitsintensiv, da Anmerkungen über Mail geschickt und Video- oder Rohschnitte über Upload-Dienste ausgetauscht werden müssen. Eine interne Abfrage in den programmerzeugenden Direktionen hatte daher einen hohen Bedarf an einem Abnahmetool mit geeignetem Funktionsumfang ergeben. Darin können die Redaktionen Anmerkungen direkt an jedem Einzelbild der Videos vornehmen.

Bei meiner Prüfung war vor allen Dingen von Interesse, was die Produktionsfirma an personenbezogenen Daten in das Tool hochladen wird. In erster Linie wird sendefähiges

Videomaterial eingespeist, das für die Publikation bestimmt ist. Denkbar ist aber auch die Verarbeitung von Login-Daten der Mitarbeiterinnen und Mitarbeiter. Denn das Usermanagement sieht Accounts mit SWR Mailadressen und den Mailadressen der Produktionsfirmen vor. Aber auch ein Arbeiten mit Funktionsaccounts ist möglich. Ich habe dem Einsatz des Tools zustimmen können. Soweit keine Funktionsaccounts genutzt werden, sind die Einwilligungen der Mitarbeitenden in die Verarbeitung der Login-Daten einzuholen. Zusätzlich wurde mit dem Toolanbieter ein Auftragsverarbeitungsvertrag geschlossen.

2.3 Auf digitaler Spurensuche – Tracking

Der SWR kann seinen gesetzlichen Auftrag nur erfüllen, wenn er weiß, ob seine Programme bei den Rundfunkteilnehmern Anklang finden und wie Verbesserungen möglich sind. Deshalb erhalte ich regelmäßig Anfragen zu einem rechtmäßigen **Einsatz von Tracking-Tools**. Dies erfolgt von den unterschiedlichsten Abteilungen, zumal es wohl kein einheitliches Werkzeug gibt. Mit den digitalen Tools ist es möglich , Spuren der Besucher der SWR-Webseiten oder der Nutzer der Apps nachzuvollziehen. Dabei darf jedoch **keine individuelle Zuordnung** zu einzelnen Nutzern möglich sein, weil es ausreicht, wenn Nutzergruppen oder allgemeine Nutzergewohnheiten festgestellt werden.

Als Beispiel lässt sich das Tool von Adjust nennen, womit die Anzahl von App-Installationen gemessen werden kann. Zunächst wurden mit dem Tool nur die **App-Installationen der ARD-Audiothek** erfasst, die über Werbeanzeigen im Netz erfolgten. Mittlerweile wird die Messung auch auf der Webseite der ARD Audiothek durchgeführt, da die App dort ebenfalls heruntergeladen werden kann. Dem Einsatz von Adjust habe ich unter der Auflage zugestimmt, dass die **Messung ausschließlich anonymisiert** erfolgt und die Nutzer der App in der Datenschutzerklärung in vollem Umfang über die Datenerhebung informiert werden. Außerdem können die Nutzer der Erfassung ihrer Daten über eine Opt-Out-Funktion widersprechen. Zudem wurde mit dem Unternehmen ein Auftragsverarbeitungsvertrag geschlossen, der die Verarbeitung der IP-Adresse als personenbezogenes Datum bis zur Anonymisierung DSGVO-konform abbildet.

Anders verhielt es sich dagegen bei der Frage der Zulässigkeit einer sogenannten **Server-To-Server-Messung** (S2S). Mit einer S2S-Messung werden Conversions über

eine **Klick-ID** (UUID) gemessen. Unter Conversions versteht man im Marketing die Umwandlung eines Status einer Zielperson in einen neuen Status. Unter einer ID versteht man eine Identifikationsnummer. Das in Frage kommende Analysetool ist von der Konzeption ein Instrument für die Analyse von Werbe- und Kaufentscheidungen und letztlich auch ein Empfehlungssystem für Unternehmen im Hinblick auf den Verkauf ihrer Produkte. Dafür generiert das Tool die Klick-ID durch Setzen eines Cookies in dem Moment, in dem der Nutzer beispielsweise auf eine Werbung des SWR klickt, die auf fremden Seiten geschaltet ist. Der Anbieter anonymisiert die IP-Adresse bei diesem Vorgang um das letzte Oktett unter Verwendung einer Geolokalisierung. Bei der daraus generierten UUID handelt es sich um eine Online-Kennung und damit um ein personenbezogenes Datum. Diese Klick-ID wird kundenseitig gespeichert und in Folge weiterer Klicks des Nutzers mit weiteren personenbezogenen Daten angereichert. Die so angereicherte UUID wird über postback-URL an den Anbieter für eine Auswertung (report) übermittelt. Diese Auswertung würde dann dem SWR als Ergebnis der Messung zur Verfügung gestellt. Dadurch käme es zu einem Austausch personenbezogener Daten und der Verarbeitung dieser Daten durch den Anbieter.

Bei näherer Betrachtung fiel auf, dass sich der Anbieter nicht nur die Weitergabe der personenbezogenen Daten, beispielsweise Bewegungsdaten, unserer Nutzer vorbehalten ließ, sondern diese Daten auch für eine lange Dauer von 13 Monaten speichern wollte. Der Anbieter wollte zwar personenbezogene Daten der SWR-Nutzer verarbeiten, sich jedoch keinen Weisungen unterwerfen und einen Auftragsdatenverarbeitungsvertrag abschließen, sondern im Gegenteil diese Daten für eigene kommerzielle Zwecke nutzen. Zudem fehlte dem Tool eine Opt-Out Funktion und die Daten werden zu lange gespeichert. In dieser praktizierten Form erfüllt der Anbieter nicht die Anforderungen der DSGVO. Das Server-to-Server-Tracking verstößt gegen die Datenschutzgrundverordnung, weshalb eine Beauftragung eines Anbieters mit einer derartigen **Server-To-Server-Messung nicht zulässig** ist.

2.4 Dauerbelastung: Auftragsverarbeitungsverträge ohne Ende

Auch im Jahr 2020 wurden wieder zahlreiche Arbeiten an Fremdfirmen vergeben. In der Regel kam es dabei zu einer Verarbeitung personenbezogener Daten, für die im Auftrag

des SWR ein sogenannter **Auftragsverarbeitungsvertrag (AV-Vertrag)** nach Artikel 28 DSGVO abzuschließen war. Hierfür existiert ein **Muster,** das die **Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten** entwickelt haben und das von meinen Mitarbeitern und mir **auch ins Englische übersetzt** worden ist. Eine Aufzählung aller Verträge würde den Rahmen meines Tätigkeitsberichts sprengen, so dass stattdessen kurz auf zwei Auftragsverarbeitungen einzugehen ist:

- Für die **kommenden Landtagswahlen** in Baden-Württemberg und Rheinland-Pfalz wird der SWR die jeweiligen Kandidaten mit Hilfe einer Online-Befragung vorstellen. Damit wird den Wählern ein **Kandidatencheck** angeboten, für den Infratest dimap als technischer Dienstleister fungiert. Eine Speicherung der sensiblen Daten der Wähler oder ein Rückschluss auf deren Identität muss dabei vermieden werden.
- Des Weiteren erforderte der **Videokonferenzbetrieb** der Cisco Telepresence Endgeräte in der **Cisco Cloud** den Abschluss einer Vereinbarung zum Datenschutz. Neben einem AV-Vertrag kamen auch Regelungen zur Informationssicherheit mit den notwendigen technischen und organisatorischen Maßnahmen sowie Standardvertragsklauseln zum Einsatz.

Ich habe die Hoffnung, dass **zukünftig** die jeweiligen Bereiche mit Hilfe der Vertragsmuster die **Vereinbarungen selbständig** (oder mit Hilfe des Justitiariats) abschließen und nur noch gelegentlich unsere Beratungskompetenz in Anspruch genommen werden muss.

2.5 ARD-Hörspieltage in Pandemiezeiten

Die diesjährigen **ARD-Hörspieltage** fanden coronabedingt unter Einschränkungen statt. Möglich war die Veranstaltung nur unter der Auflage, dass die Anzahl der Gäste über eine geringere Ticketausgabe begrenzt wurde. Für eine zügige und kostengünstige Umsetzung wurde daher beschlossen, den Anmeldeprozess der Besucher über das bereits etablierte Softwaretool „Besucherführung online“ vorzunehmen. Die notwendigen Modifikationen sollte derselbe Softwareentwickler leisten, der bereits das Tool programmiert hat. Außerdem war geplant, vor Ort eine neu entwickelte IOS-App für I-Phones einzusetzen. Die App ermöglicht es, mit dem Smartphone einen QR-Code zu scannen, der vorab mit

den Tickets an die Besucher versendet wird. Der Code kann dann direkt mit einer hinterlegten Teilnehmerliste abgeglichen werden.

Die **Erfassung von Kontaktdaten** ist über die Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2 (Corona-Verordnung – CoronaVO) möglich, da damit eine Rechtsgrundlage für die Verarbeitung der Daten gegeben ist (Erfüllung einer rechtlichen Verpflichtung). Da die Daten aber nicht ausschließlich durch den SWR verarbeitet werden und das Softwaretool **durch einen Dienstleister gehostet** wird, musste somit ein Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO geschlossen werden. Für die Verwendung des Tools Besucherführung online gab es bereits einen geschlossenen AV-Vertrag, der aber die Erfassung und Verarbeitung der Corona-Kontaktdaten nicht gänzlich abbildete. So war beispielsweise die Eintrittszeit der Teilnehmer zu den ARD-Hörspieltagen als spezielle Art persönlicher Daten (entgegen der Vorgaben der DSGVO) nicht Teil des Vertrages. Zudem war zu bedenken, dass die Corona-Verordnung gemäß § 6 Abs. 2 vorsieht, die erfassten Daten für eine Kontaktnachverfolgung vier Wochen lang aufzubewahren. Danach sind die Daten aber umgehend **vollständig zu löschen**. So müssen die Daten auf den eingesetzten Smartphones, die für das Scannen verwendet werden, wie auch bei dem Hosting-Dienstleister gelöscht werden.

2.6 Transparenz durch Datenschutzerklärungen

Für die Europäische Datenschutz-Grundverordnung (DSGVO) ist **Transparenz** ein wichtiges Prinzip. Deshalb muss auf jeder **Homepage und App** angegeben werden, welche Daten beim Aufruf dieser erhoben werden, sowie, ob und wie diese Daten genutzt werden. Informationen zu Cookies oder zur Verlinkung sind ebenso gefordert, wie der Hinweis auf die datenschutzrechtliche Verantwortlichkeit, die Darstellung der Betroffenenrechte und welches Aufsichtsorgan für Datenschutzbeschwerden zuständig ist. Dies geschieht in der Regel in der sogenannten **Datenschutzerklärung** (auch Datenschutzhinweise genannt), die nach den gesetzlichen Vorgaben mit nur ein oder zwei Klicks erreichbar sein muss. Zwar ist es sinnvoll, wenn der SWR beispielsweise auf seinen Seiten eine einheitliche Datenschutzerklärung verwendet, doch nicht für jede Webseite werden beispielsweise die gleichen Instrumente zu Reichweitenmessungen eingesetzt.

Auch die sprachlichen Anforderungen sind beim Kindernetz andere als beispielsweise bei SWR2. Da eine Homepage in der Regel einer ständigen Änderung unterworfen ist, müssen auch die entsprechenden Informationen zur Verwendung der Daten ständig aktualisiert werden. Dies bedingt eine permanente Überwachung und Beratung durch das Datenschutzdezernat. In diesem Zusammenhang sind zudem immer wieder gegenüber anfragenden Dritten die **Rechtsgrundlagen einer Reichweitenmessung** zu erläutern: Es gehört zu den gesetzlichen Aufgaben des SWR, die Bevölkerung, und zwar alle Personenkreise, mit Information und Unterhaltung zu versorgen. Ob dieser Auftrag erfüllt wird, kann wie bei der klassischen Feststellung der Reichweite und Quoten beispielsweise im Fernsehen nur durch entsprechende Messungen festgestellt werden. Für die Internetangebote geschieht dies dadurch, dass beispielsweise mit Hilfe eingebetteter Zählpixel gemessen wird, ob und welche Seiten wie lange aufgerufen werden. Rechtsgrundlage für die Reichweitenmessung ist für den SWR **Art. 6 Abs. 1 Satz 1 Ziff. c DSGVO**. Ob hier jeder Bereich sein eigenes Tool zur Reichweitenmessung braucht sei dahingestellt.

2.7 Google Firebase in der ARD-Mediathek

Zum Jahreswechsel erhielt ich die Anfrage eines Nutzers zur neu konzipierten ARD-Mediathek. Dieser hatte sich registriert und ein Konto erstellt. Dabei fiel ihm auf, dass **bei der Registrierung ein Firebase-Konto erstellt** wurde. Firebase ist ein Dienst von Google, der zur Entwicklung von Webanwendungen genutzt wird. Er hatte Sorge, seine Daten, wie z. B. E-Mailadresse und Passwort, könnten so an Google übermittelt werden. Außerdem wies er darauf hin, es fehle eine Information in der Datenschutzerklärung.

Ich bin dem Anliegen nachgegangen und habe festgestellt, dass sein Einwand berechtigt war. Es war in der Tat so, dass nicht darüber informiert wurde, dass Google Firebase als sogenannter Identitiy-Provider verwendet wurde. Auf die Information hatte man verzichtet, da die angegebenen Daten nicht von Google, sondern nur von der ARD einzusehen sind. Die Verarbeitung erfolgte im Auftrag mit einer Verschlüsselung, so dass ein Schutz der Daten gewährleistet ist. Aus Gründen der Transparenz wurde die **Datenschutzerklärung** aber umgehend **angepasst**. Insofern waren die Anmerkungen des Nutzers sehr hilfreich. Die zügige Umsetzung quittierte der Nutzer mit einem Lob für den öffentlich-rechtlichen

Rundfunk: „Ich bin immer sehr zufrieden mit den Produkten des öffentlichen Rundfunks gewesen und jetzt natürlich noch ein Stückchen mehr."

2.8 Wahl des Orchestervorstands des SWR Symphonieorchesters

In pandemischen Zeiten ist es schwierig, reguläre Wahlen stattfinden zu lassen. Aus diesem Grund erreichte mich von Seiten des Wahlausschusses die Anfrage, wie eine **Onlinewahl des Orchestervorstand** datenschutzkonform durchgeführt werden könnte. In der näheren Überlegung standen bereits mehrere Tools, darunter eine Firma mit guten Referenzen und BSI Zertifizierung.

Grundsätzlich ist eine **Onlinewahl** durchaus möglich, wenn die Wahlordnung diese Alternative vorsieht. So hat beispielsweise der Redakteursausschuss in der Vergangenheit bereits eine Onlinewahl erfolgreich durchgeführt. Bei näherer Betrachtung der **gegenwärtig geltenden Orchesterwahlordnung** fiel jedoch schnell auf, dass ausschließlich direkt oder über Briefwahl abgestimmt werden kann. Damit verblieb für diese Wahl alternativ **nur die Möglichkeit der Briefwahl**. Erst wenn zukünftig die Wahlordnung entsprechend angepasst wird, ist bei der nächsten Wahl des Orchestervorstands ist eine Onlinewahl möglich.

2.9 SWR Symphonieorchester, Corona und die Wissenschaft

Die Berliner **Charité Klinik** beabsichtigte, bei verschiedenen deutschen Berufsorchestern und Berufschören eine sog. **Langzeit-Kohortenstudie** zum Infektionsgeschehen durchzuführen. Daran wollte sich auch der SWR (nach Rücksprache mit dem Orchestervorstand) beteiligen. Im Rahmen dieser Studie sollen auch sensible personenbezogene Gesundheitsdaten der Mitglieder des **SWR Symphonieorchester** abgefragt werden, und zwar in regelmäßigen zeitlichen Abständen und auf Onlinebasis. Der Manager des SWR Sinfonieorchesters hat mir deshalb das Datenschutzkonzept der Charité zur Begutachtung übersandt. In der Folge konnten einige Unklarheiten geklärt werden. Nachdem zudem feststand, dass die Daten direkt auf Servern unter der Obhut der Charité (und nicht außerhalb Europas oder in irgendwelchen weltweiten Clouds) gespeichert werden, konnte ich meine Zustimmung geben.

2.10 WhatsApp minimieren!

WhatsApp ist auch im SWR ein datenschutzrechtliches und redaktionelles Dauerthema (vgl. Ziff. 2.2 des TB 2019). Während **WhatsApp im Verwaltungsbereich nicht zulässig** ist, weshalb z. B. darüber keine Krankmeldungen oder **keine Personaldisposition** erfolgen darf (vgl. Ziff. 3.5), ist die Situation im Programmbereich differenziert zu betrachten:

Da der SWR alle Bevölkerungsgruppen erreichen soll, muss angesichts der Verbreitung von WhatsApp auch die Möglichkeit bestehen, dass sich z. B. Zuhörer per WhatsApp an den SWR wenden und nicht nur E-Mail, Telefon oder Telefax beim SWR zum Empfang bereitstehen. Diese aus journalistischen Gründen vorhandene „**Empfangsbereitschaft**“ darf aber nicht dazu führen, dass WhatsApp durch das Programm aktiv beworben wird oder die Zuhörer aufgefordert werden, (nur) über WhatsApp mit dem SWR in Kontakt zu treten. Abgesehen davon, dass schon nach den Geschäftsbedingungen von **WhatsApp** dieser Dienst **nur von Privatkunden** genutzt werden darf, bestehen bei WhatsApp datenschutzrechtliche Mängel und Probleme:

Es findet ein ständiger **Upload von Adressbuchdaten** des Nutzers zu WhatsApp statt. Damit werden die Kontaktdaten von Personen, die noch nicht bei WhatsApp registriert sind, ohne deren Einwilligung an das Unternehmen übermittelt. Die Kontaktdaten werden dabei auf Servern von WhatsApp **in den USA gespeichert** und mit den Daten anderer Nutzer abgeglichen. Durch die Datenübermittlung in die USA besteht auch hier das Problem der Datenübermittlung ins Ausland (vgl. das EuGH-Urteil vom 16.7.2020, C-311/18 zum Privacy Shield).

Die Kommunikation bei WhatsApp mag zwar verschlüsselt sein, doch muss berücksichtigt werden, dass bei jeder Kommunikation auch **unverschlüsselt** sogenannte **Metadaten** übermittelt werden: Neben der Telefonnummer sind dies auch diverse weitere Informationen wie Geräteinformationen, Art und Häufigkeit der Nutzung, IP-Adresse oder neuerdings auch die Facebook Messenger-ID (bei gleichzeitiger Installation des Facebook Messengers). WhatsApp kann somit jederzeit nachvollziehen, wer mit wem von welchem Standort über welches Endgerät wie lange kommuniziert hat.

WhatsApp ist **Teil des Facebook-Konzerns**. Es gehört zu dessen Geschäftsmodellen, Informationen, insbesondere auch Metadaten , für werbliche Zwecke in eigener Verantwortung zu nutzen.

Wer WhatsApp auf seinem Smartphone installiert hat, benutzt häufig eine automatische **Backup-Funktion** in der Cloud oder dem Rechner. Diese ermöglicht eine einfache Wiederherstellung im Falle eines Verlustes. Der Nachteil besteht darin, dass hier **keine Verschlüsselung** erfolgt, die Chatverläufe und alle weiteren so anfallenden Daten sind damit im **Klartext** z. B. bei Google oder Apple abgelegt.

2.11 ARD Retro – Archivmaterial und Datenschutz

Seit Oktober 2020 sind in der ARD Mediathek unter dem Label „ARD Retro“ **zeitgeschichtliche Videos** für die Zeit **vor 1966** verfügbar. Ausschließlich zur privaten und nichtkommerziellen Nutzung können dort die Beiträge angesehen („gestreamt“), jedoch nicht heruntergeladen werden. Die mehr als 7.000 Produktionen umfassen zeitgenössische Berichterstattung, regionale Reportagen, lokale und nationale Nachrichtensendungen sowie Beiträge des DDR Fernsehens (in der Regel aufgrund der damaligen technischen Bedingungen in schwarz-weiß). Datenschutzrechtlich wird sich herausstellen, inwieweit einzelne Personen sich von den Sendungen in ihrem Persönlichkeitsrecht nicht nur betroffen fühlen, sondern sich auch auf die „**Gnade des Vergessens**“ berufen, also ihren **datenschutzrechtlichen Löschungsanspruch** beziehungsweise Anspruch auf eingeschränkte Verarbeitung geltend machen werden. Einen ersten, schon erledigten Fall gibt es bereits.

2.12 Augen auf bei der Partnerwahl

Der SWR hat für die **Aktion SWR1 Pfännle** eine **Kooperation mit der AOK** durchgeführt. So wurde auch ein AOK Familienfrühstück in Zusammenarbeit mit den Landfrauen organisiert. Die AOK hat dabei vor Ort ein Gewinnspiel durchgeführt, wie auch bei ihren anderen Aktionen. Dabei wurden personenbezogene Daten der Teilnehmer, unter anderem deren Kontaktdaten und Krankenkassenzugehörigkeit, erhoben. Die AOK wollte die Daten der **Gewinnspielteilnehmer** auch **zu Werbezwecken** nutzen, sofern die Teilnehmer hierzu eingewilligt hatten. Nur diese Daten sollten verwendet werden. Da

jedoch nicht die notwendigen technischen und organisatorischen Maßnahmen getroffen worden sind, wurden die Daten von mehr als 500 Gewinnspielteilnehmern ohne deren Einwilligung zu Werbezwecken verwendet. Dafür hat der baden-württembergische Landesdatenschutzbeauftragte **gegenüber der AOK ein Bußgeld** verhängt. Zwar war der SWR von der Datenschutzpanne bei der Gewinnspielaktion nicht betroffen, doch habe ich die Marketingverantwortlichen im SWR gebeten, zukünftig bei der Ausgestaltung der Kooperationsvereinbarung noch genauer darauf zu achten, dass sich die Partner datenschutzkonform verhalten.

3 Datenschutz im Verwaltungsbereich des SWR

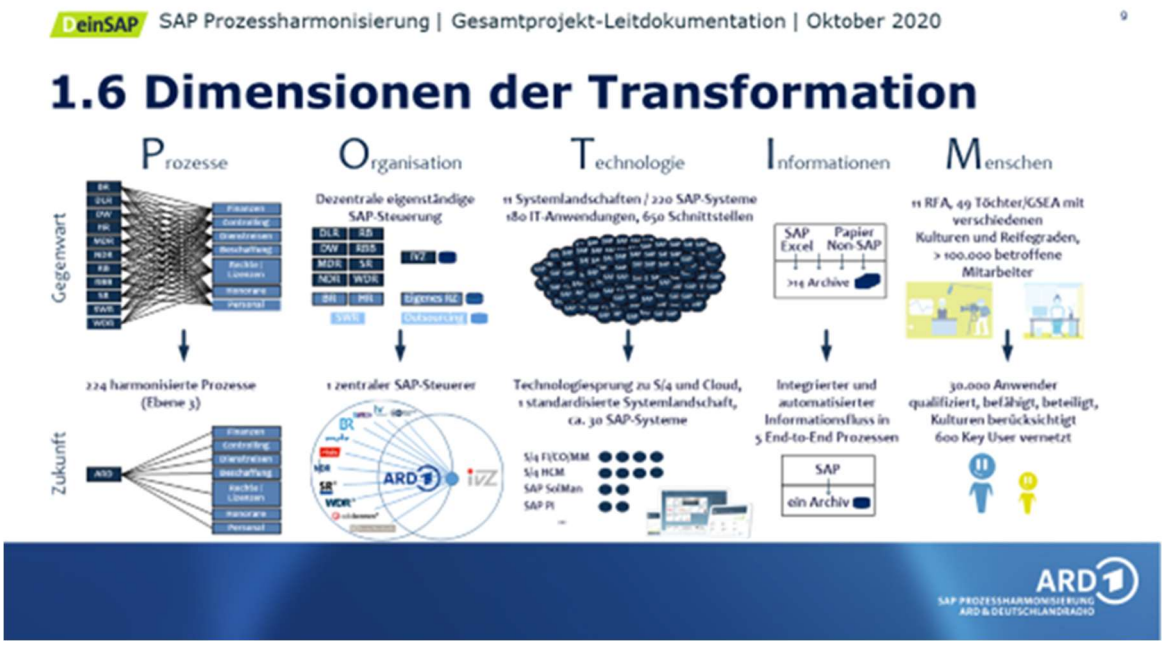
3.1 SAP-Prozessharmonisierung

Mit der am 16. April 2018 vereinbarten Kooperation zur Durchführung des Projekts „**SAP Prozessharmonisierung der ARD-Landesrundfunkanstalten und Deutschlandradio**“ wurde der Grundstein gelegt, die betriebswirtschaftlichen Prozesse und die dafür genutzten technischen Systeme im öffentlich-rechtlichen Rundfunk zu harmonisieren. An dieser Vision halten neun Rundfunkanstalten sowie das Deutschlandradio und die Deutsche Welle fest, um durch Strukturoptimierung Einsparungen auch in 49 ihrer Töchter/GSEA mit unterschiedlichen Kulturen und Reifegraden zu ermöglichen. Dazu soll eine moderne und nachhaltige S4 HANA Lösung von SAP zum Einsatz kommen, die von einem wirtschaftlichen und zentralen SAP-Steuerer, dem Informations- und Verarbeitungszentrum (IVZ), unterstützt wird.

Das **SAP-Gesamt-Projekt besteht aus 29 Einzelprojekten** mit einer Laufzeit von ca. 10 Jahren. So werden **11 Systemlandschaften, bestehend aus 220 SAP-Systemen**, 180 IT-Anwendungen und 650 Schnittstellen, zu einer standardisierten Systemlandschaft mit ca. 30 SAP-Systemen und 224 harmonisierten Prozessen transformiert. Aus 14 Einzel-Archiven wird eine gemeinsame Archivdatenhaltung. Von den über 100.000 betroffenen -Mitarbeitern und -Mitarbeiterinnen der Rundfunkanstalten (RFA) arbeiten derzeit 400 in erweiterten Teams und Gremien. Der für das intern eingesetzte RFA-Personal genutzte Gesamt-Ressourcenbedarf liegt aktuell geschätzt bei 61.500 Personen-Tagen (PT). Die Einführung der neuen technischen Systeme für zukünftig 30.000 Anwender erfolgt in zwei Clustern. **Cluster eins** beinhaltet die Module Finanzen, Dienstreisen, Controlling, Beschaffung/Vertragswesen/Warenwirtschaft und den Personal-Ministamm. **Cluster zwei** wird anschließen mit den Modulen Rechte und Lizenzen, Honorare und Personal. Die datenschutzrechtliche Prüfung dieser riesigen Projektlandschaft erfolgt in den Rundfunkanstalten nach dem Federführungsprinzip durch die jeweiligen Datenschutzbeauftragten. Allerdings entbindet mich dies nicht von der Verpflichtung und Verantwortung, alle diese Papiere zu lesen und zu prüfen, zumal SWR-spezifische Besonderheiten bestehen können. Für den SWR habe ich das Migrationskonzept mit SAP

MDC (Stammdatenkonsolidierung), dem SAP-Migration-Cockpit und SAP PI (Schnittstellenmanagement) begleitet und abgenommen.

3.1.1 Grafik SAP Gesamtprojekt-Leitdokumentation



3.1.2 SAP-Solution Manager

Das Anwendungspaket S/4 HANA von SAP besteht, vergleichbar zu Microsoft 365, aus einer Vielzahl einzelner Anwendungen. Diese Anwendungslandschaft lässt sich nur mit Hilfe eines technischen Systems betreiben. Der **SAP Solution Manager** ist das **zentrale Tool** einer darauf aufbauenden Systemlandschaft und somit ein mächtiges Werkzeug. Die Systembeschreibung des Solution Managers spricht gar von der „Werkbank“ des Gesamtsystems, mit dessen Hilfe alle SAP-Anwendungen entwickelt, getestet und schließlich rechtskonform betrieben werden sollen. Dabei kommt die sogenannte Variante „Focused Build“ zum Einsatz, die SAP gerade für große Projekte entwickelt hat, deren Nutzer an unterschiedlichen Standorten arbeiten. Die Variante bietet dafür geeignete Instrumente und vorkonfigurierte Workflows im Sinne einer „best practice“. Für die Arbeit mit den zahlreichen funktionalen Komponenten des Solution Managers weist SAP den

Rollen der Nutzer entsprechend funktionsbezogene Aufgabenprofile mit der dafür nötigen Berechtigung zu. So gibt es beispielsweise die Rolle des Projektmanagers, des fachlichen und technischen Anwendungsexperten sowie des Test und Release Managers, um nur einige Rollenbezeichnungen zu nennen.

Allein wegen der **Logdaten im System**, kommt es bereits bei der Anmeldung für die Arbeit mit dem Solution Manager zu einer Verarbeitung personenbezogener Daten.

Die nachfolgenden Datenarten werden für die Nutzung des Solution Managers verarbeitet:

- Datenart 1 – Daten zur Dokumentation von Änderungen an den verwalteten Systemen
- Datenart 2 – Daten aus der Funktion Lösungsdokumentation
- Datenart 3 – Daten zur personalisierten Selbstorganisation
- Datenart 4 – Logdaten

Bis auf die Logdaten werden die Datenarten direkt im Solution Manager gespeichert. Systembedingt erfolgt eine **Speicherung der Logdaten im SAP-Netweaver**. Der Netweaver ist das technische System, vergleichbar einem Betriebssystem, auf dem der Solution Manager betrieben wird. Die jeweiligen Datenarten dürfen nur solange aufbewahrt werden, wie ihre Speicherung für den Verarbeitungszweck erforderlich ist. Für einige Daten existieren gesetzliche Aufbewahrungsvorschriften, die einer Löschung über einen bestimmten Zeitraum entgegenstehen. So müssen beispielsweise Wirtschaftsprüfer zehn Jahre auf Nachweise zugreifen können, die die ordnungsgemäße Systementwicklung dokumentieren.

Die Datenschutzbeauftragten der Rundfunkanstalten haben bereits für die Projektphase des SAP Solution Managers ein Löschkonzept zur Voraussetzung der Nutzung gemacht. Projektseitig wurde daher ein **umfangreiches Löschkonzept** auf Basis der DIN 66398 und 66399 für die Zeit des Projektverlaufs erstellt. Für den Produktivbetrieb des Solution Managers ist geplant, die dafür ausgearbeiteten Löschregelungen in ein ganzheitliches Löschkonzept für die SAP-Systeme zu integrieren. Nach geringfügigen Anpassungen des Entwurfs konnte der SAP Solution Manager wie geplant eingesetzt werden.

3.2 Neue Kameras im Eingangsbereich und Foyer

Wir erhielten eine Anfrage, **neue Kameras** zu genehmigen, die den Haupteingang und den Innenbereich des Foyers erfassen sollten. Die in diesem Bereich vorgesehene Sanierung war der Anlass, mit dem Umbau auch neue Blickwinkel zu erschließen und damit den aktuellen **Sicherheitsbedürfnissen des SWR** gerecht zu werden. Beim Umbau wurden baulich die Voraussetzungen zur Installation dieser Kameras vorausschauend geschaffen. Bevor die Kameras installiert werden konnten, bedurfte es jedoch der Genehmigung verschiedener verantwortlicher Stellen im Haus. Aus Sicht des Datenschutzes gab es keine grundsätzlichen Einwände gegen die geplante Installation, zumal damit auch **keine Leistungs- und Verhaltenskontrolle der Mitarbeiter** bezweckt war oder ist. Eine Opposition formierte sich aber trotzdem in den Reihen der Mitarbeiter, die sich immer und überall durch ihren Arbeitgeber verfolgt und überwacht sahen. Die Kabelanschlüsse samt Projekt mussten zunächst auf Eis gelegt werden, allerdings wird der SWR, um seinen sicherheitsrelevanten Anforderungen gerecht werden zu können, eine der Kameras im ersten oder zweiten Quartal 2021 in Betrieb nehmen müssen. Es gilt, unberechtigte Personen, die sich in diesem Bereich aufhalten, zu identifizieren und am Zugang zum Gebäude zu hindern.

3.3 Parkberechtigung mit QR-Code in Baden-Baden

Für die Verbesserung der Mobilität am Standort Baden-Baden ist ein funktionierendes **Parkkonzept** von entscheidender Bedeutung. Daher soll im Zuge der Erneuerung der Schrankenanlage auch eine Säule mit **QR-Code-Reader** zum Einsatz kommen. Mit Einladungsschreiben sollen die **Gäste des SWR** bereits einen QR-Code erhalten, der es ihnen ermöglicht, an einem bestimmten Tag mit ihrem PKW einfahren und parken zu können. Der QR-Code kann entweder vom Smartphone oder als Ausdruck von einem Scanner ausgelesen werden. Im Ausnahmefall ist auch weiterhin eine Einfahrt über die Klingel vor Ort möglich. Für die Ausfahrt wird der QR-Code nicht benötigt.

Gegen das Vorhaben bestanden keine datenschutzrechtlichen Bedenken. Um den QR-Code zu generieren, kommt ein neues System zum Einsatz, das nur mit Berechtigung von einem begrenzten Personenkreis bedient werden kann. Ich habe angeregt, dass die Gäste zusätzlich zu den Schildern vor Ort auf die **Videoüberwachung der Parkflächen** des

SWR hingewiesen werden. Die für den QR-Code benötigten Angaben der Gäste werden nach vierzehn Tagen gelöscht.

3.4 Selbstaufschreibung im Projekt PS²

Ausgangspunkt für eine Selbstaufschreibung im SWR war die Situation, dass sich eine Projektgruppe bei ihrer Arbeit nicht auf eine bestehende Prozessdokumentation stützen konnte. Daher musste in diesem Bereich eine Ist-Prozess-Analyse erstellt werden. Darunter ist zu verstehen, dass die im Projekt tätigen Key-User eine Selbstaufschreibung ihrer Tätigkeiten vornehmen. Da mit einer Arbeitsdokumentation unter Umständen eine **Verhaltenskontrolle von Mitarbeitenden** möglich ist, musste somit sehr sorgfältig geprüft werden, welche Angaben nicht in dem für die Selbstaufschreibung vorgesehenen Formular enthalten sein durften.

Der mir zur Prüfung zugeleitete Entwurf einer Selbstaufschreibung enthielt neben Namensfeldern auch die Felder Direktion, Haupt-/Abteilung und Stellenbezeichnung. Nach dem **Grundsatz der Datenminimierung** dürfen aber nur solche personenbezogenen Daten abgefragt werden, die für das Erreichen des Projektziels unverzichtbar sind. An Stelle von Klarnamen kann beispielsweise auch mit Kennziffern gearbeitet werden, die den Key-Usern vorab zuzuweisen sind. Auf diese Weise sind die Daten pseudonymisiert. Besser ist es jedoch, ganz auf die Angabe von Namen zu verzichten. Doch auch solche Fragen wie „Von wem haben Sie Input erhalten?“ bzw. „An wen geben Sie Erkenntnisse weiter?“ zielen auf einen unmittelbaren Personenbezug, der für eine Prozessdokumentation nicht notwendig ist. Denn um Prozesse zu verstehen, reicht es aus zu wissen, über welchen Bereich oder Abteilung (oder Position im SWR) die Informationen erfolgen. Nach Rücksprache mit der Projektleitung wurden alle Felder entfernt, die auf einen Personenbezug abstellten.

3.5 Kabelhilfen ohne WhatsApp-Anschluss

Der Messenger Dienst WhatsApp ist weit verbreitet. Es war deshalb nicht verwunderlich, dass in einem administrativen Bereich **WhatsApp zur Disposition der Kabelhilfen** eingesetzt wurde und dann auf andere Bereiche ausgedehnt werden sollte. Damit wäre aber WhatsApp ein **Instrument der Personalplanung** und Disposition geworden, was

nicht zulässig ist. WhatsApp ist zumindest im Verwaltungsbereich ein unzulässiges Instrument. Es gibt Alternativen, wie sich auch in der Praxis gezeigt hat, nämlich die Disposition über E-Mail. Ich habe deshalb im Februar 2020 vom Einsatz von WhatsApp zur Personaldisposition dringend abgeraten. Der Bereich hat sich auch daran gehalten, so dass keine Anordnung oder förmliches Verbot ausgesprochen werden musste.

3.6 Unendlich unverständlich

Ich hatte im letzten Tätigkeitsbericht von 2019 unter Ziff. 3.1 berichtet, dass der SWR versucht hat, alle Mitarbeiterinnen und Mitarbeiter **auf die Vertraulichkeit** entsprechend den Vorgaben der DSGVO zu **verpflichten.** Am 7. Mai 2018 wurde die entsprechende Erklärung nebst Merkblatt zur Unterschrift versandt. Nachdem auch Ende 2019 immer noch 173 Mitarbeiterinnen und Mitarbeiter keine Unterschrift geleistet haben, habe ich im damaligen Tätigkeitsbericht nicht nur darauf hingewiesen, sondern auch massiv den verantwortlichen Personalbereich gebeten, aktiv zu werden. Jetzt, in den ersten Tagen des Jahres 2021, wurde mir mitgeteilt, dass es immer noch **"11 Widerspenstige"** gibt, denen eine letzte Frist bis zum 15. Februar 2021 gesetzt wurde, bevor es zu einer **Abmahnung** kommen soll. Mir fehlt jegliches Verständnis für das Verhalten dieser elf Personen, welche schließlich aus öffentlichen Rundfunkbeiträgen bezahlt werden und deshalb besonders gesetzestreu sein sollten.

3.7 Microsoft Office 365

Der amerikanische **Softwareriese *Microsoft*** bietet ein **Komplettsystem für Büroanwendungen** sowohl für Privatpersonen wie auch für Firmen und Behörden an. Das zunächst unter dem Namen Office 365, jetzt Microsoft 365 lizenzierte Softwarepaket beinhaltet z. B. die Schreibsoftware *Word*, *PowerPoint* für Präsentationen oder *Excel* als Tabellenkalkulationsprogramm. Mit *Outlook* wird auch ein E-Mail-Programm angeboten. Nachdem beim SWR die bislang eingesetzte E-Mail Software *Lotus Notes* auslief, kam man zu der Überzeugung, das **ganze Office-Paket von Microsoft** zu nehmen. Dies zumal spezielle Pakete für Firmen („Enterprise Versionen“) angeboten wurden. Darin enthalten war auch die Möglichkeit der **Speicherung in der Cloud** („*One-Drive*“) sowie die Nutzung der Plattform *Teams*, welche nicht nur für Chats, sondern auch für **Videokonferenzen** genutzt werden kann. Die Überlegungen wurden weit vor Corona angestellt und auch das

Problem der Speicherung in einer amerikanischen Cloud erörtert. Nachdem die Treuhandlösung über die Telekom nicht nur ca. 25 % teurer geworden wäre und zudem für den SWR mit Studios in der ganzen Welt und der Notwendigkeit des mobilen Arbeitens an jedem beliebigen Ort bestand, entschied man sich für einen direkten Vertrag mit Microsoft zu Office 365, zumal auch kaum alternative Produkte vorhanden sind und man deshalb meinte, auf den Quasi-Monopolisten Microsoft zurückgreifen zu müssen.

Geplant war die schrittweise Einführung und nach und nach sollten weitere einzelne Werkzeuge („*Tools*“) mit dem Gesamtpersonalrat und Datenschutzbeauftragten besprochen und eingeführt werden. Weitere Tools sind z. B. *Forms* und *Sway o*der zukünftig das Terminplanungstool *FindTime*.

3.7.1 Microsoft Forms

Mit dem **Tool *Forms*** können **Umfragen durchgeführt** werden. Das Werkzeug war aber bislang nur in Pilotprojekten im Einsatz. Auch wenn derartige Umfragen im Einzelfall sinnvoll sind, muss dafür Sorge getragen werden, dass von den Teilnehmern nur solche personenbezogenen Daten abgefragt werden, die erforderlich sind. Werden beispielsweise Erfahrungen mit bestimmten Produkten oder Verfahrensweisen abgefragt, so sind weder die Namen der Mitarbeiterinnen und Mitarbeiter noch deren konkretes Alter oder die ganz konkrete Zuordnung zu einer Redaktion und Abteilung notwendig.

3.7.2 Microsoft Sway

Das **Tool *Sway*** ist eine **Online-Webanwendung**, mit der sich **Präsentationen** bestehend aus Text und Medien erstellen lassen. Die Präsentationen können nur mit Hilfe eines Webbrowsers in einer Webanwendung von Microsoft angesehen werden. Denn die mit *Sway* erstellten Präsentationen sind auf den Servern von Microsoft gespeichert. Entgegen anderer Dienste von Microsoft, die eine Nutzung und Speicherung der Daten in der EU vorsehen und seit kurzem sogar in Deutschland ermöglichen, werden die Präsentationen mit Sway momentan **ausschließlich in den USA gespeichert**. Dies ist nach dem kürzlich ergangenen **Urteil des Europäische Gerichtshofs** (EuGH) vom Juli 2020 zum **Privacy Shield (Schrems II)** sehr problematisch. Denn der EuGH stellte in seinem Urteil fest, dass der Privacy Shield als Angemessenheitsbeschluss der Europäischen Kommission für ein

vergleichbares Datenschutzniveau der EU nicht mehr gültig ist. Microsoft stützt die davon betroffenen Datenverarbeitungen daher nicht mehr auf den Privacy Shield, sondern auf die **Standard-Vertragsklauseln**, die aber nur als geeignete Garantien für ein angemessenes Datenschutzniveau gelten, sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Nach den Ausführungen des Gerichtes fehlt es aber gerade in den USA an einer solchen Verteidigungsmöglichkeit, um sich als betroffene Person vor staatlichen Zugriffen zu schützen. Daher sind die **Standard-Vertragsklauseln nur dann** weiter anwendbar, wenn **zusätzliche Garantien** bestehen, die betroffene Personen vor staatlichem Zugriff schützen.

In den folgenden Fällen wäre eine solche **zusätzliche Garantie** zu sehen:

- Verschlüsselung, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann (Ende-zu-Ende Verschlüsselung).
- Anonymisierung oder Pseudonymisierung, bei der nur der Datenexporteur die Zuordnung vornehmen kann.

Da **für Microsoft *Sway*** derzeit **keine zusätzlichen Garantien** zur Verfügung stehen oder eine Speicherung in der EU möglich ist, habe ich darum gebeten, den Dienst **Sway** zumindest vorläufig zu **deaktivieren** und nach einer datenschutzkonformen Alternative für dieses Präsentationswerkzeug zu suchen. Dem ist die Hauptabteilung IT, Medien- und Produktionstechnik ohne Murren nachgekommen.

3.7.3 Microsoft Teams

Als der erste Lockdown im März 2020 angeordnet wurde und sich quasi ein Drittel der Mitarbeiterinnen und Mitarbeiter **im Home Office** befand, entwickelte sich eine riesige **Nachfrage**, insbesondere nach **Videokonferenzen**. Das seit Jahren bestehende ARD-Konferenzsystem des Sternpunktes in Frankfurt konnte den Ansturm kaum bewältigen und damit kam die große Stunde von Microsofts *Teams*. Allerdings müssen auch beim Einsatz dieses Tools, wie auch anderer Kollaborationssysteme, also elektronischer Plattformen, die eine **ortsunabhängige Kommunikation und Zusammenarbeit zwischen mehreren Beteiligten** ermöglichen, die datenschutzrechtlichen Anforderungen berücksichtigt werden. Mag man in Krisenzeiten wie Corona auch vorübergehend großzügig sein, so

müssen doch letztendlich die rechtlichen Rahmenbedingungen insbesondere die DSGVO eingehalten werden (vgl. auch nachfolgend Ziff. 5.1 zur Datensicherheit).
Die Rundfunkdatenschutzkonferenz (www.rundfunkdatenschutzkonferenz.de) hat deshalb Anfang 2021 **datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen** verabschiedet.

4 Datenschutz beim ARD ZDF Deutschlandradio Beitragsservice

4.1 Grundlagen zum Rundfunkbeitrag

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

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

Für die **Kontrolle** dieses Zentralen 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. 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 7,4 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.

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 (**datenschutz@beitragsservice.de**). Als Mitglied des Arbeitskreises der Rundfunkdatenschutzbeauftragten ist sie zudem ins Netzwerk der Kontrolle im Rundfunkbereich eingebunden (vgl. Ziff. 7.6).

4.2 Datenbestand beim Zentralen Beitragsservice und beim SWR

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

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

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

4.3 Meldedatenabgleich

Der letztmals im Mai 2018 durchgeführte **Meldedatenabgleich** ist jetzt **als regelmäßiges Instrument** des Beitragsservice in § 11 Abs. 5 Rundfunkbeitrags-Staatsvertrag (RBStV)

vorgesehen**.** Wie bereits im letzten Tätigkeitsbericht vermeldet, gab es dazu praktisch keine datenschutzrechtlichen Beschwerden oder Vorkommnisse.

4.4 Tücken der Telearbeit und Pannen im Home Office durch die Corona-Pandemie

Nach Ausbruch der Corona-Pandemie wurden viele Mitarbeiterinnen und Mitarbeiter des **Beitragsservice** in Köln **ins Home Office gesandt**. Um gleichzeitig die Einhaltung des Datenschutzes und der Informationssicherheit bei der Heimarbeit zu gewährleisten, wurden mit den Mitarbeitern des Zentralen Beitragsservice in Köln (ZBS) **Regelungen zum Datenschutz** getroffen. Analog wurde eine solche Zusatzvereinbarung auch mit externen Dienstleistern der telefonischen und schriftlichen Sachbearbeitung zum Arbeiten im Home Office geschlossen. Diese Regelungen waren zunächst befristet. Nachdem aber abzusehen war, dass das Virus noch weit ins Jahr 2021 seine Verbreitung finden würde, stand eine Verlängerung der Befristung zur Disposition. Die Zusage wurde davon abhängig gemacht, dass gemäß den vertraglichen Regelungen ein **Nachweis über die datenschutzkonforme Arbeitsweise** im Home Office erbracht werden musste. Bei den Mitarbeitern des ZBS konnte dagegen auf den Nachweis verzichtet werden, da eine Verbindlichkeit der Datenschutzhinweise und Sicherheitsregeln bereits über eine Dienstvereinbarung gegeben war. Zudem ist im Jahr 2021 eine neue Dienstvereinbarung zum Home Office in Planung. Eine weitergehende Sensibilisierung der Mitarbeiter findet über das Intranet und ein zusätzliches Merkblatt statt, das auf die im Home Office geltenden Datenschutz- und Sicherheitsregeln hinweist.

Dennoch kam es zu einer **Datenschutzpanne**: Für die Arbeit im Home Office wurde auch eine **Rufumleitung** vom dienstlichen Apparat auf die private Telefonnummer eingerichtet. Dabei hat sich dann schnell herausgestellt, dass bei einem Anruf von Dritten der Anrufer in bestimmten Fällen auch die private Telefonnummer der Mitarbeiter sehen konnte. Dies führte dazu, dass Mitarbeiter auch **auf ihren privaten Nummern direkt angerufen** wurden. Nachdem dies festgestellt worden war, wurde unverzüglich durch technische Maßnahmen dafür Sorge getragen, dass zukünftig bei einer Rufumleitung die private Telefonnummer der Mitarbeiter des Beitragsservice nicht mehr angezeigt wird.

4.5 Vereinbarung zur gemeinsamen Verantwortlichkeit („Joint-Controllers“)

Alle Landesrundfunkanstalten sowie das Deutschlandradio des ZDF sind für die **Verarbeitung der Rundfunkteilnehmerdaten** im Rahmen des Rundfunkbeitragseinzugs bzw. der Rundfunkbeitragsbefreiung **gemeinsam verantwortlich**. Es wurde deshalb im Jahre 2020 gemäß Art. 26 EU-DSGVO von den Intendanten eine **Vereinbarung zur gemeinsamen Verantwortlichkeit** (sog. Joint Controller Agreement) abgeschlossen. Aus ihr ergibt sich beispielsweise, wer die aus der DSGVO resultierenden Verpflichtungen zu erfüllen hat, wie die Datenschutzaufsicht organisiert wird bzw. wie die gegenseitigen Verantwortlichkeiten und Meldewege bei Informationen sowie eventuellen Datenpannen sind.

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 (Amtsgericht Gütersloh, HRB 10100). Paigo hieß früher „infoscore Forderungsmanagement GmbH“ und ist Teil der Firmengruppe „Arvato Financial Solutions“ und gehört zum Bertelsmann-Konzern. 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 Kundenkontakt-Management

Der Beitragsservice in Köln (die frühere GEZ) ist für den Einzug des Rundfunkbeitrags, einschließlich notweniger Mahnmaßnahmen sowie auch der Verwaltung der Millionen

befreiten Rundfunkbeitragszahler, verantwortlich. Es sind täglich zehntausende von eingehenden Schreiben oder Meldungen vom Umzug bis zur Änderung des Bankkontos zu verarbeiten. Dies gilt sowohl für private wie auch für nicht private Teilnehmer (z. B. Unternehmen oder öffentliche Stellen sowie Behörden). Für die **nicht privaten Teilnehmer** bietet der Beitragsservice bereits jetzt die Möglichkeit, **Änderungen direkt im Teilnehmerkonto** einzugeben (z. B. im Hinblick auf Standorte von Firmen oder Änderungen der Mitarbeiterzahl). Es können auch die Daten zu den Zahlungen sowie der jeweilige Kontostand abgerufen werden.

Jetzt soll auch den **privaten Rundfunkteilnehmern** ein **Self-Service** über das Internet angeboten werden, zumal über das Online-Zugangsgesetz des Bundes entsprechende Voraussetzungen bestehen und auch immer mehr Behörden, Kommunen und staatliche Einrichtungen eine elektronische Kommunikation anbieten. Durch die Pandemie wurde dies nochmals verstärkt und erhielt einen neuen Schub. Die Kommunikation zwischen einem Rundfunkteilnehmer und dem Beitragsservice erfordert jedoch eine Identifizierung und **Authentifizierung**, d. h. es muss sichergestellt sein, dass derjenige der Änderungen im Teilnehmerkonto vornimmt, auch der Inhaber des Teilnehmerkontos ist. Hier sind derzeit verschiedene Möglichkeiten in der Überlegung, um zu einer dokumentierten Einwilligung zu kommen. Das Projekt soll möglichst in 2021 abgeschlossen werden.

4.8 EUDAGO

In den letzten Zügen liegt derzeit ein riesiges Projekt des Beitragsservice, nämlich die **finale Umsetzung der EU-Datenschutz-Grundverordnung** (DSGVO).

Personenbezogene Daten, die nicht mehr benötigt werden, sind zu löschen, es sei denn, es bestehen **Aufbewahrungsvorschriften** (z. B. aufgrund von handels- oder steuerrechtlichen Normen); in diesem Fall sind die Daten zu sperren, was bedeutet, dass nur ein sehr eingeschränkter Personenkreis (in der Regel die Wirtschaftsprüfer) darauf zugreifen können. 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 (§ 20 Abs. 3 Nr. 3 BDSG alte Fassung sowie § 35 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.

Bereits im Vorgriff auf die DSGVO war das Projekt EUDAGO vom Beitragsservice aufgesetzt worden, um alle rechtlichen Anforderungen umzusetzen. Das Projekt wurde von mir als Mitglied des Controlboards, (stellvertretend für alle Datenschutzaufsichtsorgane) begleitet. Ziel war und ist es, automatisiert alle nicht mehr benötigten Daten unter Berücksichtigung der gesetzlichen **Löschungspflichten**, aber **auch** der **Aufbewahrungsvorschriften**, zu beseitigen. Das Problem dabei ist, dass fast alle gespeicherten Informationen einen Buchhaltungsbezug haben und deshalb bei einer Löschung Fehler im Teilnehmerkonto entstehen können. Seit Gründung der GEZ existierte ein Großrechnersystem, welches effizient war und die Bearbeitung der inzwischen auf über 41 Millionen angewachsenen Teilnehmerkonten im Online-Verfahren erlaubte. Das seit 1976 gewachsenes System stand immer wieder vor Herausforderungen, weil zum Beispiel sowohl die Umstellung der Postleitzahl von vierstellig auf fünfstellig, als auch der gesamtdeutsche Gebühreneinzug 1990 jeweils einen Programmieraufwand von über 20 Personenjahren erfordert hatte. Deshalb war auch das **Löschprojekt EUDAGO** eine große Herausforderung. Es gelang aber trotz der großen Verflechtungen der Teilnehmerkonten und der buchhalterischen Anforderungen in Löschläufen zum Ende des Jahres 2020 eine gesetzeskonforme Situation zu erreichen. So wurden insbesondere alte Buchhaltungsdaten oder erledigte Befreiungen (die nur noch logisch vorhanden waren und einem sehr eingeschränkten Zugriff unterlagen) erfolgreich gelöscht.

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 Multi-Faktor-Authentifizierung (MFA) für Office 365 bzw. Microsoft 365

Der Zugriff auf einen Rechner oder eine Anwendung nur mit einem Benutzernamen und einem Passwort ist heutzutage nicht mehr **Stand der Technik**. Notwendig ist ein **weiteres Sicherheitselement**. Dies kann beispielsweise darin bestehen, dass nach dem Einloggen am Rechner mit Nutzer-ID und Passwort auf ein vorher vom Nutzer festgelegtes Telefon, Smartphone oder über eine Smartphone-App eine Nummer generiert wird, welche der Benutzer dann zusätzlich eingeben muss. Erst dann kann die Anwendung genutzt werden. Um den Zugang zu Microsoft 365 (ehemals Office 365) sicher zu gestalten und vor Missbrauch zu schützen, wurde deshalb zum Jahresanfang diese so genannte **Multi-Faktor-Authentifizierung** beim SWR eingerichtet.

Der E-Mailabruf über die Mail-App mit dem dienstlichen iPhone/iPad funktioniert nach wie vor wie gewohnt. Die Nutzung von Microsoft 365 Applikationen (z. B. Outlook, OneDrive oder Teams) auf dem dienstlichen iPhone/iPad und generell die Nutzung von Office 365 auf privaten Endgeräten ist jetzt **nur noch mit** der **Multi-Faktor-Authentifizierung** möglich.

5.2 Datensicherheit im Home Office, nicht nur in Corona Zeiten

Als im Frühjahr 2020 die Covid-19-Pandemie zum Lockdown führte, arbeiteten immer mehr Mitarbeiterinnen und Mitarbeiter beim SWR **im Home Office**. Dies bedeutet auch für die Datensicherheit **zusätzliche Gefahrenmomente**. So muss nicht nur ausgeschlossen werden, dass andere Personen in einer Wohnung Zugriff auf dienstliche Daten haben, sondern auch die Datenträger (oder etwaige Papierunterlagen) müssen geschützt und von privaten Rechnern getrennt werden. Ein geschützter Pfad der Daten von den SWR-Rechnern auf die Rechner zu Hause (in der Regel durch Verschlüsselung)

ist notwendig und es muss vermieden werden, dass die „ankommenden Daten“ über ein ungeschütztes WLAN im Home Office (statt einer kabelgebunden Verbindung) auf dem Dienstgerät „ankommen“. Die Verarbeitung von Daten hat möglichst in der Weise zu erfolgen, dass die betroffenen Mitarbeiterinnen und Mitarbeiter die Daten vom SWR erhalten bzw. sich im Einzelfall „holen“, danach die Verarbeitung vornehmen und dann die Daten wieder auf SWR-Rechner zurück übermitteln. Der PC zu Hause soll damit im Wesentlichen nur wie ein „dummes“ Terminal genutzt werden. Durch die Speicherung auf den zentralen SWR-Rechnern ist für die Betroffenen auch das **Problem des Back-ups**, also der Datensicherung, gelöst. Ergänzend ist darauf hinzuweisen, dass der SWR bereits 2017 einen Tarifvertrag vereinbart hatte.

Unabhängig davon, und noch vor Corona, gab es 2020 einen **speziellen Fall von Home Office**. Da die Ehefrau eines SWR-Mitarbeiters eine **Arbeitsstelle in Fernost** angenommen hatte, wollte er sie begleiten und dann von dort aus im Wege der Telearbeit seine arbeitsvertraglichen Pflichten erfüllen. Da der Mitarbeiter im Wesentlichen planerische Aufgaben zu erfüllen hat und damit sowohl von der Art als auch vom Umfang nur weniger kritische Daten bezieht, konnte mit ihm eine entsprechende Vereinbarung geschlossen werden, welche auch die oben geschilderten Punkte zur Datensicherheit enthielt. Der aufgrund meines Vorschlags abgeschlossene Vertrag mit dem Mitarbeiter enthielt indessen **nicht** das in meinem Entwurf enthaltene **Kontrollrecht des SWR vor Ort**.

Zum **Home Office beim Zentralen Beitragsservice** siehe Ziff. 4.4.

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

Im September 2020 wurde wieder über die RBT, die Arbeitsgemeinschaft Rundfunk-Betriebstechnik von ARD, ZDF und Deutschlandradio, ein **Penetrationstest**, also quasi ein simulierter Angriff durchgeführt. Er ergab, dass keine Schwachstellen gefunden wurden, welche eine Übernahme von Systemen oder Anwendungen des SWR ermöglichen würden. Soweit **kleinere Schwachstellen** in Form einer fehlenden oder unzureichenden Konfiguration der Verschlüsselung bei Systemen festgestellt wurden, wurden diese danach **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). Gleichwohl hat die KEF Informationen zu den Kosten der Datensicherheit und zu den Datenschutzbeauftragten angefordert. Sie hat nicht berücksichtigt, dass es nur einen Datenschutzbeauftragten gibt und damit unzulässigerweise personenbezogene Daten (insbesondere über das Gehalt) angefordert werden.

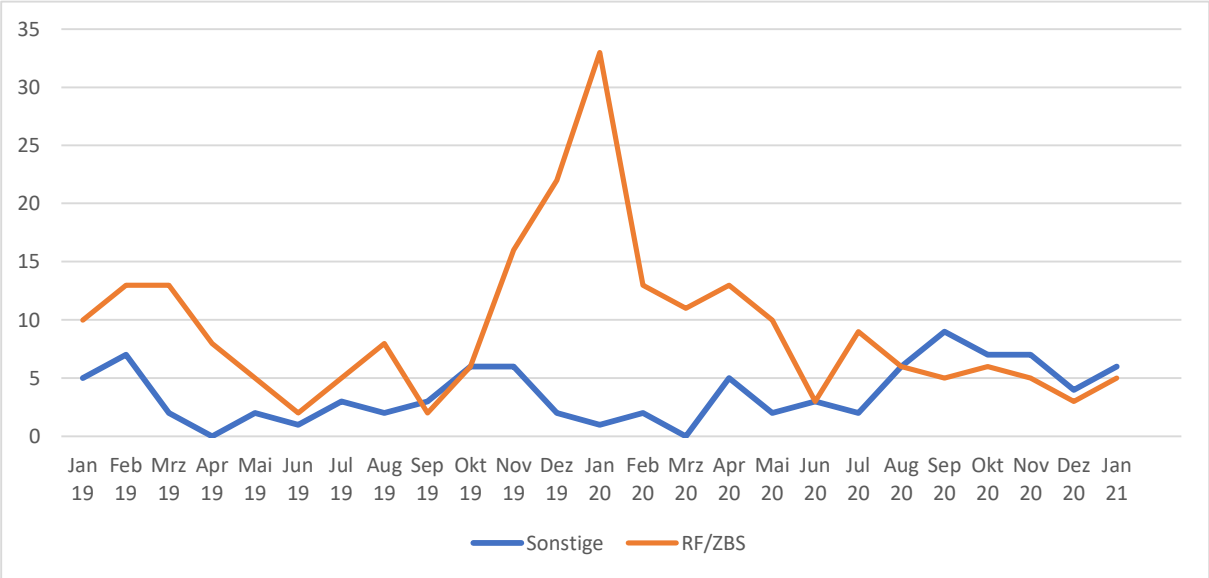
6. Auskunftsersuchen und Beschwerden

Bei den Auskunftsersuchen sowie Beschwerden über vermeintliche Datenschutzverstöße ist es wie bei der Corona-Pandemie: Sie **kommen in Wellen**. 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** direkt an mich bzw. den SWR sind 2020 nicht nur wieder **gestiegen**, sondern auch vielfältiger, differenzierter und **im Einzelfall schwieriger** zu bearbeiten und zu beantworten gewesen. Durch die Pandemiesituation bestand eine zusätzliche Schwierigkeit: Viele der Beschwerden kommen 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 einem abgelegenen Untergeschoss residiert, hatte dies zumindest den Vorteil, dass praktisch keine Kontakte mit anderen (bis auf die Poststelle) vorhanden stattfanden.

Mit insgesamt **166 Beschwerden und Auskunftsersuchen im Jahr 2020** war wieder gegenüber 2019 (147 Beschwerden) ein Anstieg von über 12 % zu verzeichnen, der mir große personelle Sorgen bereitet. Die beiliegende Übersicht zeigt den Eingang im **Monatsverlauf der Jahre 2019 und 2020**:



6.1.1 Direkteingaben zum Rundfunkbeitragseinzug

Von den insgesamt 166 Beschwerden, die bei mir im Jahr 2020 eingingen, betrafen **117** 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 auch in diesem Jahr, die sich 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 2020 pandemiebedingt nur noch bei einem Drittel der Eingaben erreicht werden.

6.1.2 Sonstige Direkteingaben beim Rundfunkdatenschutzbeauftragten

Die **Eingaben und Beschwerden** ohne jeglichen Bezug zum Rundfunkbeitragseinzug nehmen kontinuierlich zu und haben sich beispielsweise von 24 auf 48 im Jahr 2020 **verdoppelt**. Die Mehrzahl dieser Petenten zeichnet sich durch eine **kritische Begleitung der Programme** des SWR aus, insbesondere der 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.
- Eine große Resonanz fand das im Jugendprogramm *funk* angebotene **Computerspiel www.reichstag-defender.de**. Hier wurde nach dem Sturm auf den Reichstag im August 2020 ein als Satire gedachtes Spiel produziert und angeboten, bei welchem jeder Spieler seinen Erfolg bei der Abwehr von Angriffen auf den Reichstag testen konnte. Viele Petenten empfanden dieses Spiel als Verunglimpfung und „subversives Machwerk".
- 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** oder **Instagram** 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.
- Schließlich gab es zwei Fälle, bei denen von den Petenten zu Recht gerügt wurde, dass im Rahmen der **Corona-Berichterstattung** über die Situation auf den **Intensivstationen in den Krankenhäusern**, nicht die notwendige journalistische Sorgfalt angewendet worden ist. Denn in beiden Fällen wurde auch ein Schwenk auf den Monitor eines Intensivpatienten gemacht und dort konnte man mit nur geringem Aufwand deren Namen und Geburtsdaten lesen. Ich habe die verantwortlichen Hauptabteilungsleiter gebeten, für eine entsprechende Sensibilisierung ihrer Mitarbeiterinnen und Mitarbeiter zu sorgen, da es ein Leichtes ist, diese **Daten zu verpixeln** oder sonst unkenntlich zu machen.

6.2 Anfragen und Auskunftsersuchen beim Beitragsservice in Köln

Inzwischen ist es **beim Zentralen Beitragsservice** in Köln fast zur Routine geworden, die zahlreichen Auskunftsersuchen zu beantworten. Die Zahl dieser **Auskunftsersuchen** ist aber **2020 mit 33.379** im Vergleich zu den 10.417 im Jahr 2019 wieder **beträchtlich**

gestiegen. Die Frage, welche personenbezogenen Daten jeweils gespeichert sind, wird aber regional unterschiedlich gestellt. Im Süden der Republik ist der Anteil höher und **besonders signifikant** sind die Zahlen für den **SWR**. Ob es an Querdenkern oder besonders kritischen Geistern liegt, vermag ich nicht zu beurteilen. Tatsache ist aber, dass es keine Rundfunkanstalt gibt, die so viele Auskunftsersuchen zu verzeichnen hat. Die **6.153 Auskunftsersuchen** von Rundfunkteilnehmer des **SWR** sind sowohl absolut als auch prozentual einsame Spitze.

7 Organisation und Zusammenarbeit bei der Datenschutzkontrolle

7.1 Aufbau und Organisation auf europäischer Ebene

Die **EU-Datenschutz-Grundverordnung** sieht die Errichtung von **Aufsichtsbehörden** vor (in der alten Richtlinie 95/46/EG „Kontrollstellen“ genannt). In den **Artikeln 51 ff. EU-DSGVO** werden hierzu konkrete Vorgaben gemacht. Die Aufsichtsorgane müssen **unabhängig** sowie **weisungsfrei** sein und keiner Dienst-, Fach- oder Rechtsaufsicht unterliegen.

Aufgrund der durch die DSGVO geschaffenen Stellung und der dort zugewiesenen Aufgaben zur Umsetzung von grundlegendem europäischen 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 EU-DSGVO), der weitreichende Aufgaben und Befugnisse hat.

7.2 Aufbau und Organisation in Deutschland

Nach der **EU-Datenschutz-Grundverordnung** (Art. 51 Abs. 1 EU-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 EU-DSGVO),
- die **Rundfunkdatenschutzbeauftragten** sowie
- die Datenschutzbeauftragten bei den Landesmedienanstalten.

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

7.3 Aufbau und Organisation bei den Rundfunkdatenschutzbeauftragten

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

7.4 Zusammenarbeit aller Aufsichtsbehörden auf nationaler Ebene

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

Mit der **Geltung der EU-DSGVO** sind nicht nur deren **Regelungen zur Zusammenarbeit** zu beachten, sondern im neuen, ab 25. Mai 2018 geltenden BDSG vom 30. Juni 2017

(BGBl. 2017, S. 2097), wird in **§ 16 Abs. 5 BDSG** die Bundesdatenschutzbeauftragte verpflichtet, auf die Zusammenarbeit mit denjenigen Stellen hinzuwirken, die für den Datenschutz in den Ländern zuständig sind. Zudem **verpflichtet § 18 BDSG** die Aufsichtsbehörden des Bundes und der Länder **zur Zusammenarbeit**. Aus Art. 51 Abs. 2 EU-DSGVO und dem Erwägungsgrund 119 ergibt sich, dass **alle Aufsichtsbehörden gleichwertig** und damit **gleich zu behandeln** sind. Eine Klassifizierung z.B. nach Größe (z.B. des Bundeslandes) oder Kontrollbereichen (z.B. öffentlich-rechtlich) ist nicht zulässig. Auch die Aufsichtsbehörden nach Art. 85 EU-DSGVO (Medien) sowie Art. 91 EU-DSGVO (Kirchen) sind **gleichwertige Aufsichten** nach Art. 51 Abs. 2 EU-DSGVO.

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

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

Nicht einmal in die **Unterarbeitsgruppen** der DSK ist eine Aufnahme als vollwertiges Mitglied erfolgt. In die Informationsflüsse, insbesondere aus dem Europäischen Datenschutzausschuss (Art. 68 EU-DSGVO), sind die öffentlich-rechtlichen Rundfunkanstalten vom Bundesdatenschutzbeauftragten nach wie vor **nicht eingebunden**.

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

7.5 Zusammenarbeit der Datenschutzbeauftragten auf Länderebene

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

7.6 Konferenz und Arbeitskreis der Rundfunkdatenschutzbeauftragten

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 Telefonschaltungen bzw. in Sondersitzungen beraten. Auch der Datenschutzbeauftragte des Österreichischen Rundfunks (ORF) nimmt regelmäßig an den Sitzungen teil. Der Arbeitskreis bietet Gelegenheit, Erfahrungen auszutauschen und anstaltsübergreifende Projekte gemeinschaftlich und zielgerichtet datenschutzkonform

abzuwickeln. Hier werden auch die Interessen und Meinungen im Sinne der Mitwirkung bei gesetzgeberischen Vorhaben im Medien- und Datenschutzbereich gebündelt. Seit 1.1.2019 liegt der Vorsitz bei Herrn Dr. Heiko Neuhoff (NDR) und Herr Stephan Schwarze (MDR) ist sein Stellvertreter.

7.6.2 Rundfunkdatenschutzkonferenz (RDSK)

Um die Zusammenarbeit im Hinblick auf die **aufsichtsrechtlichen Befugnisse,** insbesondere nach **Art. 58 EU-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). 2020 lag der Vorsitz wie beim AK DSB bei Herrn Dr. Heiko Neuhoff (NDR) und als Stellvertreter Herr Stephan Schwarze (MDR). 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.

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: Empfehlungen der RDSK aufgrund des Urteils des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer).

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 (neuen) **Landesdatenschutzgesetz Baden-Württemberg** (LDSG BW) vom 12. Juni 2018 (GBl. BW, S. 173 ff.; 2019, 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. Denn während beim Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten aufgrund der EU-Datenschutz-Grundverordnung nicht nur die Zahl der Planstellen erhöht wurde, sondern auch deren Vergütung, bewirkte die **DSGVO** beim SWR **keine Änderungen**. Dabei wurden ansonsten im SWR allein in der obersten Tarifgruppe 11 neue Planstellen geschaffen.

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**).

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 (EU-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 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 wird auf **www.swr.de/datenschutz** veröffentlicht und kann als Papierdruck angefordert werden. Der **Bericht** ist aufgrund Art. 59 EU-DSGVO in § 27 Abs. 10 Satz 2 LDSG BW **jetzt jährlich zu erstatten** und zudem gilt: „Der Bericht wird den **Landtagen** und den **Landesregierungen** der unterzeichnenden Länder des Staatsvertrages über den Südwestrundfunk **übermittelt**.“

8.5 Tatkräftige Unterstützung

Bei der Erfüllung der 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.

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 gültig seit 01.01.2014

9.2 § 9c Rundfunkstaatsvertrag (RStV) in der Fassung des 21. Rundfunkänderungs-Staatsvertrages; gültig vom 25.5.2018 bis 6.11.2020
§§ 12 und 23 Medienstaatsvertrag (MStV); gültig ab 6.11.2020

9.3 § 27 Landesdatenschutzgesetz Baden-Württemberg (LDSG BW) vom 12.6.2018 (GBl. BW 2018, S. 173 ff.); gültig seit 21.6.2018

9.4 Liste der Datenschutzbeauftragten als Aufsichtsbehörden von ARD, ZDF, Deutsche Welle und Deutschlandradio im Jahre 2019

9.5 Empfehlungen der Rundfunkdatenschutzkonferenz (RDSK)

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 Sonderregelungen („Medienprivileg“). Diese waren für die Zeit vom 25. Mai 2018 bis zum 6. November 2020 in § 9c und § 57 **Rundfunkstaatsvertrag (RStV)** geregelt, der als Landesgesetz erlassen worden war (GBl. BW 2018, S. 129 ff.; auch abgedruckt im Anhang zum 12. Tätigkeitsbericht). **Jetzt** sind diese Regelung 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 2019, 1549, 1551).

§ 27
Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz

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

den Rundfunkrat mit Zustimmung des Verwaltungsrats. Die zweimalige Wiederernennung ist zulässig.

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

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

(4) Das Amt der oder des Rundfunkbeauftragten für den Datenschutz kann nicht neben anderen Aufgaben innerhalb des Südwestrundfunks und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt der oder des Rundfunkbeauftragten für den Datenschutz zu vereinbaren sein und dürfen ihre oder seine Unabhängigkeit nicht gefährden. Das Amt endet mit Ablauf der Amtszeit, mit Rücktritt vom Amt oder mit Erreichen des gesetzlichen oder tarifvertraglich geregelten Renteneintrittsalters. Die oder der Rundfunkbeauftragte für den Datenschutz kann ihres oder seines Amtes nur enthoben werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Rundfunkrats auf Vorschlag des Verwaltungsrats; die oder der Rundfunkbeauftragte für den Datenschutz ist vor der Entscheidung zu hören.

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

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

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

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

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

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

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

Rundfunkanstalten	Datenschutzaufsicht	Anschrift
BR	Dr. Reinhart Binder kontakt@rundfunkdatenschutz.de	Marlene-Dietrich-Allee 20 14482 Potsdam
Deutsche Welle	Thomas Gardemann datenschutz@dw.de	Kurt-Schumacher-Straße 3 53113 Bonn
Deutschlandradio	Dr. Reinhart Binder kontakt@rundfunkdatenschutz.de	Marlene-Dietrich-Allee 20 14482 Potsdam
Hessischer Rundfunk	Ulrich Göhler datenschutz@hr.de	Bertramstraße 8 60320 Frankfurt
Mitteldeutscher Rundfunk	Stephan Schwarze rundfunkdatenschutz@mdr.de	Kantstraße 71-73 04275 Leipzig
Norddeutscher Rundfunk	Dr. Heiko Neuhoff datenschutz@ndr.de	Rothenbaumchaussee 132 20149 Hamburg
Radio Bremen	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 Empfehlungen der Rundfunkdatenschutzkonferenz (RDSK):

RDSK
RUNDFUNKDATENSCHUTZKONFERENZ

Empfehlungen der RDSK
Folgerungen aus dem Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II“)

Mit Urteil vom 16.07.2020 (Az: C-311/18) hat der EuGH den Beschluss 2016/1250 der Kommission über die Angemessenheit des vom EU-US Datenschutzschild (Privacy Shield) gebotenen Schutzes für unwirksam erklärt. Damit kann das Privacy Shield Abkommen nicht mehr als Grundlage für Datenübermittlungen in die USA herangezogen werden. Die EU-Standardvertragsklauseln sind nach Auffassung des Gerichtshofs hingegen weiterhin gültig. Er hat jedoch betont, dass sowohl der verantwortliche Datenexporteur als auch der Datenimporteur prüfen muss, ob das gemäß den Standardvertragsklauseln unionsrechtlich geforderte Schutzniveau in dem Drittland, in das Daten übermittelt werden, überhaupt eingehalten werden kann oder ob zusätzliche Garantien geschaffen bzw. vereinbart werden müssen. Nähere Hinweise zu den gegebenenfalls erforderlichen weiteren Maßnahmen/Garantien enthält das Urteil nicht.

Diese Entscheidung stellt jeden Verantwortlichen in Europa vor die große Schwierigkeit, wie weiterhin Daten in die USA übermittelt werden können, ohne gegen geltendes Recht zu verstoßen. Die RDSK sieht die Politik und insbesondere die Europäische Kommission in der Pflicht, mit den USA ein neues Abkommen auszuhandeln, das den Anforderungen des europäischen Datenschutzrechts vollumfänglich entspricht.

Der Europäische Gerichtshof hat festgestellt, dass die Aufsichtsbehörden verpflichtet sind, eine Übermittlung personenbezogener Daten an ein Drittland auszusetzen oder zu verbieten, wenn sie der Auffassung sind, dass der nach dem Unionsrecht erforderliche Schutz nicht anders gewährleistet werden kann. Der Gerichtshof hat keine Übergangsfrist zugelassen.
Der RDSK ist bewusst, dass die Rundfunkanstalten nicht unmittelbar die Datenflüsse in Drittländer, insbesondere die USA stoppen können. Jedoch sind sie nach der Entscheidung des EuGH verpflichtet, die Datenübermittlungen an Drittstaaten, insbesondere die USA auf

den Prüfstand zu stellen und wo immer notwendig weitere Maßnahmen, wie nachfolgend skizziert, zu ergreifen.

Die RDSK empfiehlt den Verantwortlichen insoweit folgendes Vorgehen:

1. Das EU-US Privacy Shield ist nicht mehr gültig, weshalb eine allein darauf fußende Datenübermittlung in die USA rechtswidrig ist. Die Rundfunkanstalten sind vor einer weiteren Datenübermittlung im Sinne der folgenden Ziffern aufgerufen, andere Rechtsgrundlagen für die Datenübermittlung zu finden, geeignete technische Maßnahmen zu ergreifen und/oder nach einer Alternative für die jeweilige Datenverarbeitung zu suchen.
2. Der EuGH hat die Gültigkeit der Standardvertragsklauseln nicht beschränkt. Er hat jedoch darauf hingewiesen, dass auf Seiten der Verantwortlichen eine Prüfpflicht ebenso besteht wie bei dem Empfänger der Daten. Diese bezieht sich darauf, ob zusätzliche Garantien geschaffen bzw. vereinbart werden müssen, um das in den Standardvertragsklauseln geforderte Schutzniveau auch tatsächlich zu erreichen. Der Verantwortliche sollte im ersten Schritt eine Bestandsaufnahme der Datenübermittlung in Länder außerhalb des europäischen Wirtschaftsraumes und insbesondere in die USA durchführen. Eine Neubewertung der jeweiligen Datenverarbeitung ist angezeigt hinsichtlich ihrer Art, des Umfangs, des Zwecks der Verarbeitung sowie der vorgesehenen Empfänger. Maßgeblich für die Bewertung muss dabei der risikobasierte Ansatz sein, der die DSGVO prägt. In Hinblick auf die zu ergreifenden Maßnahmen kommt es also z. B. darauf an, ob nur wenige und vergleichsweise unkritische Daten in dem Drittland verarbeitet werden.

   Bei Verwendung der Standardvertragsklauseln sollte der Verantwortliche den Empfänger der Daten (Datenimporteur) auffordern, offenzulegen ob und in ggf. welcher Weise er Auskunftspflichten gegenüber US-Behörden oder Geheimdiensten unterliegt. Im Ergebnis hat der Verantwortliche zu beurteilen, ob diese Eingriffe im Lichte der europäischen Gesetzgebung als verhältnismäßig anzusehen sind. Zu berücksichtigen hat er auch, ob der Datenimporteur zusichert, ihn über einen etwaigen Zugriff durch US-Behörden zu informieren und gegen unverhältnismäßige Zugriffe rechtlich vorzugehen.
3. Zu prüfen hat der Verantwortliche überdies, ob durch geeignete technische ggf. auch organisatorische Maßnahmen ein Zugriff der US-Behörden verhindert werden kann.

Hier kommen insbesondere wirksame Verschlüsselungstechniken wie Ende-zu-Ende-Verschlüsselungen in Betracht.

4. Die Angemessenheitsbeschlüsse der EU-Kommission sind in den Blick zu nehmen. In diesen Beschlüssen wird festgestellt, dass personenbezogene Daten in einem bestimmten Drittland einen mit dem europäischen Datenschutzrecht vergleichbaren Schutz genießen. Unter folgendem Link sind die betroffenen Länder einzusehen: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de
   Eine Verlagerung der Datenübermittlung und –verarbeitung in diese Länder ist unkritisch.
5. Die Feststellungen des Gerichtes beziehen sich allein auf den EU-US Privacy Shield sowie die Standardvertragsklauseln. Daher bleiben alle weiteren von der DSGVO vorgesehenen Garantien des Artikel 46 DSGVO weiterhin anwendbar. Insbesondere können eigenständige Vertragsklauseln vereinbart werden, die jedoch von der Genehmigung der jeweils zuständigen Datenschutzaufsicht abhängig sind.
6. Ausnahmsweise kann auch eine Datenübermittlung in Drittstaaten gemäß Artikel 49 DSGVO gerechtfertigt sein. Voraussetzung ist eine nur gelegentliche und nicht wiederholte Übermittlung. Dies ist schon dann nicht der Fall, wenn die Datenübermittlung im Rahmen einer dauerhaften Vertragsbeziehung stattfindet. Hierzu gibt es eine Auslegungshilfe des Europäischen Datenschutzausschusses (https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_de).

Die RDSK weist darauf hin, dass es sich bei dieser Empfehlung um eine erste Einschätzung handelt, die sie je nach Entwicklung der Rechtslage aktualisieren wird.

Stand: August 2020

10 Stichwortverzeichnis

AK DSB 52, 53
Aufsichtsbehörden 49, 50, 51, 55, 62
Auftragsverarbeitungsvertrag 18, 20, 21
Auskunftsersuchen 45, 47, 48
Beitragsservice 36, 37, 38, 39, 40, 41, 43, 45, 46, 48
Berichtsturnus 56
Cookies 9, 13, 19, 22, 47, 53
Datenschutzaufsicht 11, 39, 41, 49, 63, 66
Datenschutzbeschwerden 22, 37
Datensicherheit 6, 42, 43, 44
DSK 51, 52, 53
Einwilligung 16, 25, 40
EUDAGO 41
Europäischer Datenschutzausschuss ... 8, 49, 52, 55, 66
gespaltene Kontrolle 50
Home Office 3, 5, 6, 34, 38, 42, 43, 45
IP-Autostart 53
Kommission zur Ermittlung des Finanzbedarfs (KEF) 44
Landesdatenschutzgesetz 36, 54, 57, 60
Logdaten 29
Löschung 29, 41, 46
Medienprivileg 14, 48, 57, 58, 59
Meldedatenabgleich 37, 38, 39, 40
RDSK 53, 64
Rundfunkbeitrag 36
Rundfunkstaatsvertrag 57, 58
Scorewerte 47
Telearbeit ..... *Siehe* Home Office
WhatsApp 24, 25, 31, 47