Tätigkeitsbericht

des Datenschutzbeauftragten des

Hessischen Rundfunks

Ulrich Göhler

für den Zeitraum

01. Januar 2020 bis 31. Dezember 2021

Gliederung:

Zusammenfassung 3

1. Vorbemerkung/Organisation 4

2. Entwicklung des Datenschutzrechts....5

2.1 Europa 5

2.1.1 EU-Datenschutz-Grundverordnung (EU-DSGVO)....5

2.1.2 Entwurf zur Neuregelung der E-Privacy-Verordnung....5

2.1.3 EuGH Urteil zum Privacy Shield („Schrems II“) 5

2.1.4 EU – Standardvertragsklauseln....7

2.1.5 Brexit 7

2.2 Bundesrecht 8

2.2.1 IT-Sicherheitsgesetz 2.0 8

2.2.2 TTDSG 9

2.2.3 Urteil des BGH v. 28.05.2020 zur Cookie-Einwilligung....9

2.2.4 Urteil des OVG Schleswig Holstein vom 25.11.2021 zur Untersagung des Betriebs einer Facebook Fanpage (s. auch: EuGH vom 05.06.2018, BVerwG vom 11.09.2019)....10

3. Datenschutz im Hessischen Rundfunk 11

3.1 Allgemeines/Verwaltung 11

3.1.1 Datenschutz beim ARD-Sternpunkt....11

3.1.2 Datenschutz im Bereich Telemedien....12

3.1.3 Cloud-Computing 14

3.1.4 Drittanbieter/Datentransfer in Drittländer 15

3.1.5 Einrichtung eines zentralen Servicedesk‘....16

3.1.6 Einrichtung einer zentrale Endgeräte-Datenbank....18

3.1.7 Etablierung einer Cloud-Security Plattform 19

3.1.8 Neuer Virenscanner 20

3.1.9 Einführung Microsoft 365 21

3.2 Datenschutz im Programm- und Produktionsbereich 23

4. Datenschutz beim Rundfunkbeitrag 28

Fragen mit direktem Hessen- bzw. hr-Bezug 30

5. Arbeitskreis der Datenschutzbeauftragten ARD/ZDF/ Deutschlandradio (AK DSB) 31

6. Rundfunkdatenschutzkonferenz (RDSK) 32

Zusammenfassung

- Obwohl das Hessische Datenschutzgesetz einen Tätigkeitsbericht des Datenschutzbeauftragten des Hessischen Rundfunks nicht vorsieht, wird seit Mitte 2006 ein Tätigkeitsbericht erstellt und auf den Internetseiten des Hessischen Rundfunks veröffentlicht.
- Wie in den Vorjahren habe ich im Berichtszeitraum wieder eine Reihe von Stellungnahmen zu hr-internen Projekten und Verfahrenserweiterungen abgegeben. Auch wurden „Verzeichnisse von Verarbeitungstätigkeiten" gemäß Artikel 30 DSGVO (früher: Verfahrensverzeichnisse gemäß § 6 HDSG alt) neu erstellt und dem Personalrat im Rahmen der Mitbestimmung vorgelegt.
- Das Wirksamwerden der Datenschutzgrundverordnung (DSGVO) zum 25.05.2018 stellt auch den Hessischen Rundfunk weiterhin vor große Herausforderungen. Für die Umsetzung der aus der DSGVO resultierenden Anforderungen ist nach wie vor ein erheblicher personeller und zeitlicher Aufwand erforderlich. Aufgrund des Umfangs der auch in Zukunft anstehenden Tätigkeiten sowie weiter bestehender „Unklarheiten" aufgrund noch fehlender Rechtsprechung und/oder entsprechender Umsetzungshinweise wird dieser Aufwand wohl auch weiterhin geleistet werden müssen.
- Das Aufkommen an Auskunftsbegehren nach Artikel 15 DSGVO ist im Vergleich zum letzten Tätigkeitsbericht rückläufig. Gleichwohl wird der Hessische Rundfunk nach wie vor (mehr oder weniger freundlich) aufgefordert, eine entsprechende Datenauskunft zu erteilen. Oft handelt es sich um „standardisierte" Schreiben, die fast alle ähnliche Texte aufwiesen und innerhalb der in Artikel 12 Abs. 3 DSGVO vorgesehenen Frist von vier Wochen bearbeitet werden konnten.
- Der Arbeitskreis Datenschutzbeauftragte ARD/ZDF/DLR (AK DSB) ist weiterhin ein wesentlicher Baustein bei der Koordinierung und Abstimmung der rechtlichen Bewertungen von durchzuführenden Datenschutzmaßnahmen der Landesrundfunkanstalten.
- Darüber hinaus erfolgt ein Austausch zu Themen der Rundfunkdatenschutzaufsicht im Rahmen regelmäßig durchgeführter Sitzungen bzw. Videokonferenzen der RDSK, dem Zusammenschluss der Rundfunkdatenschutzbeauftragten von ARD, ZDF und Deutschlandradio.

1. Vorbemerkung/Organisation

In Anwendung von § 28 Abs. 3 HDSIG und in Übereinstimmung mit der bisher geübten Praxis wird beim Hessischen Rundfunk sowohl die Funktion des betrieblichen Datenschutzbeauftragten als auch die des für den journalistischen Bereich zuständigen Datenschutzbeauftragten von mir in Personalunion ausgeübt. Ich nehme diese Aufgabe neben meiner Tätigkeit als Mitarbeiter der Internen Revision wahr.

An dieser Stelle möchte ich meiner Stellvertreterin, Frau Simone Schlee, - die im Übrigen auch tatkräftig bei der Erstellung dieses Berichts mitgewirkt hat - erneut ausdrücklich und herzlichst für Ihre hervorragende Arbeit, die konstruktive und intensive Zusammenarbeit sowie die damit einhergehende Unterstützung danken. Ohne diese Unterstützung und Ihre fachliche Expertise wäre es weitaus schwieriger, den Herausforderungen des Datenschutzes im Hessischen Rundfunk gerecht zu werden.

Analog der Verfahrensweise der Vorjahre wird dieser Tätigkeitsbericht vorgelegt und im Internet veröffentlicht, obwohl das HDSIG seit 1986 einen solchen Bericht des Datenschutzbeauftragten des Hessischen Rundfunks nicht mehr vorsieht.

Der vorliegende Tätigkeitsbericht betrifft den Zeitraum vom 1. Januar 2020 bis 31. Dezember 2021. Es werden darin allgemeine Entwicklungen des Datenschutzes sowie auszugsweise datenschutzrechtlich relevante Veränderungen und Problemstellungen im Hessischen Rundfunk während des Berichtszeitraums dargestellt.

2. Entwicklung des Datenschutzrechts

2.1 Europa

2.1.1 EU-Datenschutz-Grundverordnung (EU-DSGVO)

Seit dem 25.08.2018 gilt die DSGVO in allen Mitgliedstaaten der Europäischen Union. Das EU-Parlament hat im Rahmen einer Evaluation nach rund dreijähriger Geltungsdauer der DSGVO mit Entschließung vom 21.03.2021 festgestellt, dass die Regelungen dieser Verordnung positiv zu bewerten sind und damit den Bewertungsbericht der EU-Kommission vom 24.06.2020 bestätigt. Ein grundlegender Änderungs – oder Anpassungsbedarf wurde weder seitens des EU-Parlaments noch der EU-Kommission festgestellt. Die Ausführungen zur DSGVO im letzten Bericht haben daher nach wie vor Bestand.

2.1.2 Entwurf zur Neuregelung der E-Privacy-Verordnung

Die bislang geltende e-Privacy-Richtlinie enthält Vorgaben zur Vertraulichkeit der Information und zum Schutz der Privatsphäre im Bereich der Telemedien. Im letzten Bericht wurde festgehalten, dass das ursprüngliche Vorhaben der EU-Kommission, eine unmittelbar geltende neue e-Privacy -Verordnung zeitgleich mit der DSGVO in Kraft zu setzen, gescheitert ist. Bis heute gibt es keine Einigung auf eine entsprechende Neuregelung. Dies ist aus datenschutzrechtlicher Sicht überaus bedauerlich, da die letzte Überarbeitung der e-Privacy-Richtlinie aus dem Jahr 2009 datiert und sich in der Zwischenzeit Rechtsunsicherheiten, u.a. zu den eingesetzten Technologien im Bereich der Telemedien, wie Onlineseiten und Apps, ergeben haben. Beispielhaft sei hier der Einsatz von Cookies, u.a. für die Online-Nutzungsmessung genannt.

2.1.3 EuGH Urteil zum Privacy Shield („Schrems II")

In seinem Urteil vom 16.07.2020 (C-311/18) hat der EuGH den auf dem EU-USA-Abkommen Privacy Shield basierenden Angemessenheitsbeschluss der EU-Kommission nach Art 45 DSGVO in Bezug auf das Datenschutzniveau in den USA mit sofortiger Wirkung für ungültig erklärt.

Der EuGH hat mit diesem Urteil betont, dass personenbezogene Daten von EU-Bürgern nur dann in ein Land außerhalb des Geltungsbereiches der

DSGVO übermittelt werden dürfen, wenn dieses sogenannte Drittland ein mindestens mit der DSGVO vergleichbares Datenschutzniveau gewährleistet. Für die USA wurde dies verneint, was u.a. mit den weitgehenden Zugriffsrechten von US-Sicherheitsbehörden auf in die USA übermittelte Daten und unzureichenden Rechtsschutz für die von einer Datenverarbeitung Betroffenen begründet wurde.

Dies bedeutet, dass sich Unternehmen/Institutionen bei der Übermittlung personenbezogener Daten z.B. aus Deutschland in die USA nicht mehr auf einen Angemessenheitsbeschluss nach Art 45 DSGVO berufen können, sondern eine solche Übermittlung außer in den begrenzten Ausnahmefällen nach Art 49 DSGVO nur möglich ist, wenn geeignete Garantien für die Datenverarbeitung im Drittland vorliegen. Diese können gemäß Artikel 46 Absatz 2 lit. c) DSGVO in der Verwendung von EU-Standardvertragsklauseln bestehen. Deren Wirksamkeit hat der EuGH in seinem Urteil grundsätzlich bestätigt.

Gleichzeitig betont der EuGH die Verantwortung des Datenexporteurs, das Datenschutzniveau der Länder zu überprüfen, in die er Daten übermittelt. Dies führt dann am Beispiel der USA dazu, dass neben der Vereinbarung von EU-Standardvertragsklauseln im Zweifel ergänzende Garantien durch weitere vertragliche, technische und /oder organisatorische Maßnahmen erforderlich sind. Der EuGH hebt zudem die Rolle der datenschutzrechtlichen Aufsichtsbehörden bei der Kontrolle solcher Datentransfers hervor.

Die Auswirkungen dieses Urteils sind erheblich, da viele Standardanwendungen zur Datenverarbeitung von US-Herstellern stammen, technischer Support oftmals nach dem sogenannten „follow-the-sun-Prinzip“[1] aus verschiedenen Drittländern heraus erbracht wird und im Falle von Cloud-Dienstleistungen typischerweise Datenübermittlungen auch in Drittländer nicht gänzlich auszuschließen sind.

Zwar gibt es mittlerweile Empfehlungen zum weiteren Vorgehen für verantwortliche Stellen, u.a. vom EDSA[2] und der RDSK[3]. Diese sind jedoch eher allgemein gehalten, weshalb für jede Datenübermittlung in ein Drittland eine Einzelfallprüfung erfolgen muss. Dies verursacht bei den Verantwortlichen und auch bei den betrieblichen/behördlichen Datenschutzbeauftragten

[1] Wenn für technische Komponenten/Dienstleistungen ein Support über 24 Stunden am Tag, an 7 Tagen die Woche erforderlich ist, wird dieser beim follow-the-sun-Prinzip aus Ländern der verschiedenen Zeitzonen heraus erbracht.

[2] EDSA = Europäischer Datenschutzausschuß

[3] RDSK = Konferenz der Rundfunkdatenschutzbeauftragten als spezifische Datenschutzaufsichtsbehörden

einen nicht zu unterschätzenden Aufwand, verbunden mit einer nach wie vor bestehenden Rechtsunsicherheit, da aufgrund der weitreichenden Auswirkungen des Urteils noch nicht sämtliche Detailfragen als gelöst betrachtet werden können.

2.1.4 EU – Standardvertragsklauseln

Mit Durchführungsbeschluss (EU) 2021/914 der EU-Kommission vom 04.06.2021 hat die EU-Kommission neue Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer[4] verabschiedet. Diese neuen Standardvertragsklauseln sind für die Einbeziehung in Neuverträge seit dem 27.09.2021 verbindlich, für Altverträge gilt eine Übergangfrist für die Umstellung bis zum 27.12.2022. In Bezug auf die Aussagen aus dem Schrems II Urteil (siehe Abschnitt 2.1.3) ändert sich durch die neuen Standardvertragsklauseln nichts Wesentliches. Dies bedeutet, dass auch bei Anwendung der neuen Klauseln für die Datenübermittlung z.B. in die USA geprüft werden muss, ob weitere Maßnahmen zur Schaffung geeigneter Garantien nach Art. 46 DSGVO erforderlich sind. Die neuen EU-Standardvertragsklauseln sind für verschiedene in Frage kommenden Konstellationen von Datenübermittlungen modular aufgebaut. Für die hier besonders relevante Konstellation der Übermittlung vom Verantwortlichen an einen Auftragsverarbeiter decken die neuen Klauseln die vertraglichen Anforderungen aus Art. 28 DSGVO für die Auftragsverarbeitungsvereinbarung ab, so dass künftig im Falle einer Vereinbarung der EU-Standardvertragsklauseln kein zusätzlicher Auftragsverarbeitungsvertrag abgeschlossen werden muss.

2.1.5 Brexit

Zum 31.01.2020 ist Großbritannien aus der EU ausgetreten. Damit ist das Vereinigte Königreich datenschutzrechtlich zu einem sogenannten „Drittland“ geworden. Nach entsprechenden Übergangsvereinbarungen hat die EU-Kommission am 28.06.2021 einen Angemessenheitsbeschluss gemäß Art. 45 DSGVO erlassen, wodurch das Vereinigte Königreich als sicheres Drittland anerkannt wird. Der Erlass des Angemessenheitsbeschluss wurde von durchaus kritischen Stimmen, u.a. des Europäischen Datenschutzausschusses, begleitet. So wurden z.B. Bedenken geäußert, ob der

[4] „Drittland“ = Land, das weder den Vorschriften der DSGVO unterfällt, noch dem Europäischen Wirtschaftsraum (EWR) angehört (z.B. USA, China, Russland, Indien etc.)

Datentransfer von Großbritannien in andere Drittländer im Sinne der DSGVO ausreichend geregelt ist. Gleichwohl können nun, solange der Angemessenheitsbeschluss gültig ist, auf dessen Basis personenbezogene Daten z.B. aus Deutschland ohne weitere vertragliche oder technisch-organisatorische Hürden ins Vereinigte Königreich übermittelt werden.

2.2 Bundesrecht

2.2.1 IT-Sicherheitsgesetz 2.0

Nach längerem Vorlauf trat im Mai 2021 das IT-Sicherheitsgesetz 2.0[5] in Kraft. Zur Erhöhung der Sicherheit informationstechnischer Systeme werden die Befugnisse des Bundesamtes für Informationssicherheit (BSI) gestärkt und Rechte und Pflichten für die Betreiber kritischer Infrastrukturen erweitert. Auch wenn der Hessische Rundfunk als öffentlich-rechtliche Landesrundfunkanstalt nicht Adressat dieses Gesetzes ist, so betrachtet er die Gewährleistung der IT-Sicherheit und damit die Aufrechterhaltung der Sendefähigkeit gleichwohl als Bestandteil der Erfüllung seiner staatsvertraglichen Aufgaben. Die öffentlich-rechtlichen Rundfunkanstalten engagieren sich deshalb auch im Branchenarbeitskreis Medien des UP KRITIS, einer öffentlich-privaten Kooperation zum Schutz kritischer Infrastrukturen in Deutschland.

Auch auf Ebene der EU laufen die Beratungen zur Verabschiedung der Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union, kurz NIS 2, und einer neuen Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen.

Es ist in den letzten Jahren und Monaten eine spürbare Zunahme von Angriffen auf IT-Systeme, auch auf die von Medienhäusern, zu verzeichnen. Somit wird die Etablierung von Sicherheitsmaßnahmen zur Gefahrenabwehr und Stabilisierung von IT-Systemen immer wichtiger, und zwar auch für den Schutz der verarbeiteten personenbezogenen Daten, den der Verantwortliche gemäß Art. 32 DSGVO sicherzustellen hat. Da solche Maßnahmen mit entsprechenden Kosten verbunden sind, müssen die wachsenden Anforderungen in diesem Bereich auch bei der Ermittlung des Finanzbedarfs der öffentlich-rechtlichen Rundfunkanstalten berücksichtigt werden.

[5] „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme"

2.2.2 TTDSG

Das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) ist am 01.12.2021 in Kraft getreten. Darin werden die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) zusammengefasst und harmonisiert. Außerdem werden die Anforderungen an den Schutz vor Eingriffen in Endgeräte von Verbrauchern gemäß der geltenden e-Privacy-Richtlinie nunmehr nahezu wortgleich umgesetzt, nachdem die bisherigen Regelungen dazu in § 15 TMG alt zunehmend für Rechtsunsicherheit sorgten. Es geht dabei im Wesentlichen um Technologien wie z.B. das Setzen von Cookies beim Betrieb von Onlinediensten oder dem Einsatz von Identifiern beim Betrieb von Apps. Geschützt wird durch das Gesetz die Integrität des Endgerätes eines Nutzers vor unerlaubten Zugriffen. Dies bedeutet, dass der Begriff der „Information" zwar auch personenbezogene Daten erfasst, aber weiter zu verstehen ist. Gemäß § 25 TTDSG ist das Speichern von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, in der Regel nur zulässig, wenn der Endnutzer hierin wirksam eingewilligt hat. Von einer Einwilligung kann nur in Ausnahmefällen abgesehen werden, etwa wenn der Zugriff auf die Speicherung der Information im Endgerät des Endnutzers unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Da die öffentlich-rechtlichen Rundfunkanstalten Telemedienangebote betreiben, sind auch sie von den gesetzlichen Regelungen des TTDSG betroffen. Beim Einsatz von Cookies, local storage Elementen, Identifiern und vergleichbaren Technologien in den Telemedienangeboten muss daher in jedem Einzelfall geprüft werden, ob etwa das Cookie für die Zurverfügungstellung des Dienstes unbedingt erforderlich ist. Andernfalls sind die Voraussetzungen für die Einholung einer wirksamen Einwilligung zu überprüfen und umzusetzen. Da das Gesetz erst Ende des Jahres 2021 in Kraft getreten ist, gibt es zwar erste Auslegungsmaterialien, etwa die „Orientierungshilfe der (staatlichen) Aufsichtsbehörden für die Anbieter*innen von Telemedien ab dem 01.12.2021", aber noch keine Rechtsprechung zu der Frage, was in der Regel als „unbedingt erforderlich" angesehen werden kann. Auch die RDSK befasst sich aktuell mit dieser Frage in Bezug auf die von ihr beaufsichtigten öffentlich-rechtlichen Rundfunkanstalten.

2.2.3 Urteil des BGH v. 28.05.2020 zur Cookie-Einwilligung

Der BGH hatte in diesem Verfahren bereits 2017 Fragen zur Auslegung des Unionsrechts in Bezug auf die Wirksamkeit einer Einwilligung in das Setzen von Cookies durch ein vorangekreuztes Kästchen vorgelegt. Der EuGH hatte hierzu mit Urteil vom 01.10.2019 entschieden, dass diese Praxis den Anforderungen an die Einholung einer wirksamen Einwilligung nicht entspricht, sondern eine aktive Handlung des Nutzers erforderlich ist. Der BGH hat sodann in seinem Urteil vom 28.05.2020 auf Basis dieser Vorgaben aus dem EuGH Urteil entschieden, dass die Einwilligung in das Setzen von Cookies mittels eines bereits voreingestellten Ankreuzkästchens eine unangemessene Benachteiligung der Nutzer darstelle und damit unwirksam sei. Eine derartige Einwilligung sei mit dem wesentlichen Grundgedanken des § 15 Abs. 3 Satz 1 TMG nicht vereinbar. Denn § 15 Abs. 3 Satz 1 TMG sei i.S. der EU-e-privacy-Richtlinie dahingehend auszulegen, dass im Falle von nicht notwendigen Cookies eine wirksame Einwilligung einzuholen sei und die Einwilligung vom Nutzer aktiv, etwa durch Setzen eines Hakens/Ankreuzen erteilt werden müsse. Seit dem 01.12.2021 ist dies nun durch das TTDSG ausdrücklich gesetzlich geregelt (siehe Abschnitt 2.2.2).

2.2.4 Urteil des OVG Schleswig Holstein vom 25.11.2021 zur Untersagung des Betriebs einer Facebook Fanpage (s. auch: EuGH vom 05.06.2018, BVerwG vom 11.09.2019)

Der zugrundeliegende Sachverhalt dieses Urteils beginnt schon im Jahr 2011. Damals hatte die zuständige Aufsichtsbehörde der Wirtschaftsakademie Schleswig-Holstein den weiteren Betrieb seiner Facebook-Fanpage untersagt. Begründet wurde dies damit, dass Facebook bei Aufruf der Fanpage auf personenbezogene Daten der Internetnutzer zugreife, ohne dass diese hinreichend über Art, Umfang und Zwecke der Erhebung sowie ein Widerspruchsrecht gegen die Erstellung eines Nutzungsprofils für Zwecke der Werbung oder Marktforschung unterrichtet würden. Gegen diesen Bescheid klagte die Wirtschaftsakademie zunächst mit Erfolg vor dem zuständigen Verwaltungsgericht. Vorgetragen wurde dabei u.a., dass Facebook für die Datenverarbeitung verantwortlich sei und der Fanpage-Betreiber diese nicht beeinflussen könne. Im Verlaufe des weiteren Rechtsstreits wurden im Rahmen des Revisionsverfahrens vor dem Bundesverwaltungsgericht verschiedene Fragen, insbesondere zur Verantwortung des Fanpage-Betreibers für die bei Facebook stattfindende Datenverarbeitung, zur Entscheidung an den EuGH vorgelegt. Dieser hatte mit Urteil vom 05.06.2018 entschieden, dass der Fanpage-Betreiber Mitverantwortung für die bei Facebook stattfindende Datenverarbeitung trage, da er durch die sogenannte Insights-Funktion bei Facebook statistische Daten zur Nutzung seiner Fanpage erhalte. Hiernach

hob das BVerwG am 11.09.2019 das Berufungsurteil auf und verwies die Sache zurück an das OVG Schleswig-Holstein. In der Entscheidung vom 25.11.2021 hat das OVG Schleswig-Holstein u.a. festgestellt, dass für bestimmte Datenverarbeitungsvorgänge bei Facebook, hier insbesondere die Erstellung der Insights-Statistiken, zum maßgeblichen Zeitpunkt keine Rechtsgrundlage vorgelegen habe, da Nutzer über diese Zwecke nicht informiert worden seien. Eine Mitverantwortlichkeit der Wirtschaftsakademie wurde bejaht. Das OVG Schleswig Holsein hat unter Berücksichtigung der zuvor ergangenen Entscheidungen des EuGH und des BVerwG nun der Berufung der Aufsichtsbehörde stattgegeben.

3. Datenschutz im Hessischen Rundfunk

Auch für die zwei zurückliegenden Jahre kann ich den in meinen vorhergehenden Tätigkeitsberichten geäußerten positiven Eindruck erneut bestätigen, dass bei innerhalb des Hessischen Rundfunks auftretenden datenschutzrechtlichen Fragestellungen überwiegend eine frühzeitige Einbindung des Datenschutzbeauftragten erfolgt.

Diese frühzeitige Einbindung wird u. a. durch die seit Jahren praktizierte direkte Mitarbeit und Beteiligung des Datenschutzbeauftragten in den unterschiedlichsten Projekt-, Arbeits- und Lenkungsgruppen sichergestellt. Auch durch die von mir selbst durchgeführten Schulungen zum Thema Datenschutz wird das im hr vorhandene Datenschutzbewusstsein weiter gestärkt bzw. ständig in Erinnerung gerufen.

Die im Folgenden exemplarisch aufgeführten Einzelfälle werden analog der in meinen letzten Tätigkeitsberichten gewählten Darstellungsweise getrennt nach den Bereichen „Allgemeines/Verwaltung“ sowie „Programm- und Produktionsbereich“ betrachtet und zeigen die Bandbreite der zu bearbeitenden Themen auf.

3.1 Allgemeines/Verwaltung

3.1.1 Datenschutz beim ARD-Sternpunkt

Der ARD-Sternpunkt ist eine rechtlich nicht selbstständige Gemeinschaftseinrichtung von ARD und Deutschlandradio mit Sitz in Frankfurt, die technische Dienstleistungen für die Gemeinschaft erbringt. Da dies auch Tätigkeiten gemeinschaftlich veranlasster Datenverarbeitungen umfasst, haben die

Rundfunkanstalten der ARD und Deutschlandradio einen Joint Controller Vertrag[6] abgeschlossen. Der Vertrag sieht auch die Bestellung eines Datenschutzbeauftragten für den ARD Sternpunkt vor. Da dies aufgrund der Etatvorgaben der Gemeinschaftseinrichtung im Berichtszeitraum noch nicht umgesetzt werden konnte, erfolgte eine Beratung und Kontrolle durch die Datenschutzbeauftragten des Hessischen Rundfunks. So fanden im Berichtszeitraum u.a. spezielle Einweisungen zu den Themen Auftragsverarbeitung und Datentransfer in Drittländer statt. Konkret begleitet wurden in diesem Zusammenhang z.B. Aufträge für die Wartung der Firewall oder Dienstleistungen zur Vermeidung von DDoS-Attacken[7]. Soweit erforderlich wurden in die Verträge EU-Standardvertragsklauseln einbezogen und es wurden weitere technische und organisatorische Maßnahmen zum Schutz der Daten ergriffen, wie z.B. europäische Speicherlösungen, Einsatz von Verschlüsselungstechnologien oder die Anweisung, Fehlermeldungen nach dem Gesichtspunkt der Datensparsamkeit zu erstellen. Begleitet wurden zudem Teststellungen für Lösungen zur Erhöhung der IT-Sicherheit, an denen mehrere Rundfunkanstalten teilnahmen. Die Teststellungen wurden insbesondere im Umfeld der Bundestagswahl im September 2021 genutzt, da hier verstärkt mit Angriffen, gerade auch auf die Berichterstattung, zu rechnen war. Die datenschutzrechtliche Beratung fand hier insbesondere zu Fragen der Schutzbedarfsanalyse, Log-Daten-Verarbeitung sowie zur korrekten Einbindung von Experten statt.

3.1.2 Datenschutz im Bereich Telemedien

Im Telemedienbereich führte die BGH-Rechtsprechung vom 28.05.2020 (siehe Ziffer 2.2.3) zu einer Anweisung der Datenschutzbeauftragten hinsichtlich einer eingehenden Prüfung der eingesetzten Cookies und verwandten Technologien auf den Onlineangeboten und den Apps des Hessischen Rundfunks. Dies wurde auch zum Anlass genommen, die Verhältnisse zu einzelnen Drittanbietern wiederholt zu überprüfen und daraufhin Anpassungen an den Datenschutzinformationen bzw. bei der sogenannten Zwei-Klick-Lösung vorzunehmen. Gerade im Bereich der Telemedien hat sich die

[6] Artikel 26 DSGVO verlangt den Abschluss einer Vereinbarung, wenn zwei oder, wie hier, mehrere Verantwortliche gemeinsam die Mittel und Zwecke einer Datenverarbeitung festlegen und somit gemeinsam Verantwortliche sind. In der Praxis hat sich für diese Vereinbarungen der englische Begriff „Joint Controller“ durchgesetzt.

[7] DDoS-Attacken = Distributed Denial of Service-Attacken: ein Server wird dezentral von mehreren Systemen gezielt so stark mit Anfragen bombardiert, dass er seine Leistungen nicht mehr erbringen kann und zusammenbricht.

Etablierung eines Datenschutz-Koordinators als äußerst wichtig erwiesen. Dieser sorgt in Abstimmung mit der Datenschutzbeauftragten u.a. dafür, dass die Mitarbeitenden des Bereichs dafür sensibilisiert werden, in Frage kommende Drittanbieter vor einem Einsatz genauer dahingehend zu überprüfen, ob die Dienstleistungen DSGVO-konform erbracht werden. Dies führte dann auch dazu, dass einzelne Anbieter inzwischen nicht mehr eingesetzt werden. Gleichwohl bleibt die Überprüfung und Überwachung von Drittanbietern in diesem Bereich eine Daueraufgabe, da sich regelmäßig Geschäftsmodelle oder auch zugrundeliegende Vertragsbedingungen ändern.

Auf den Einsatz eines Cookie-Management-Fensters konnte im Berichtszeitraum verzichtet werden, da neben Cookies zum Seitenaufbau, für Einstellungen zur Barrierefreiheit oder Einstellungen des Nutzers (Sprache, Schriftgröße, Teilnahme an Umfragen o.ä.) keine personenbezogenen Trackingtools z.B. für Werbung/Marketing eingesetzt werden. Es findet lediglich eine anonymisierte Nutzungsmessung der einzelnen Angebote statt, die zur Erfüllung des staatsvertraglichen Auftrages einer öffentlich-rechtlichen Rundfunkanstalt als erforderlich zu betrachten ist, da hierüber die Auffindbarkeit oder auch Relevanz von journalistischen Beiträgen ermittelt werden kann.

In Bezug auf die Präsenz des Hessischen Rundfunks auf Drittplattformen ist festzustellen, dass die Verbreitung von Inhalten dort gemäß § 30 Absatz 4 Medienstaatsvertrag gestattet ist, wenn dies zur Erreichung der Zielgruppe aus journalistisch-redaktionellen Gründen geboten ist. Aufgrund unzählbarer Desinformationskampagnen in den sozialen Netzwerken, z.B. zum Thema Corona, ist das Argument, als öffentlich-rechtliche Rundfunkanstalt gerade auch hier faktenbasierte Inhalte zur Verfügung stellen zu müssen, nachvollziehbar. Dabei ist aus datenschutzrechtlicher Sicht allerdings zu bemerken, dass die Datenverarbeitung bei einigen Plattformen für die Nutzer zumindest intransparent ist und sich auch die allgemeinen Nutzungsbedingungen der Plattformen einschließlich der Datenschutz-Bestimmungen regelmäßig ändern. Da die Anstrengungen von ARD und ZDF mit Facebook eine individuelle Joint Controller-Vereinbarung abzuschließen, bisher nicht erfolgreich waren, wurden die Rundfunkanstalten dazu angehalten, in gesonderten Datenschutzinformationen für die Präsenz auf Drittplattformen auf ihre Verantwortung für die Datenverarbeitung einzugehen und die Lage so transparent wie möglich darzustellen. Außerdem wurde darauf hingewirkt, die Präsenz auf den verschiedenen Plattformen zu überprüfen. Im Falle des im Jahr 2020 neu aufgekommenen Dienstes Clubhouse veröffentlichte die RDSK eine Entschließung, in der aufgrund datenschutzrechtlicher Bedenken von der Nutzung des Dienstes abgeraten wurde. Im Hessischen Rundfunk wurden auf dieser Basis besondere interne Vorgaben zur Nutzung im

redaktionellen Bereich unter Beteiligung des Datenschutzbeauftragten aufgestellt.

Aufgrund der unterschiedlichen Gestaltung der Nutzungsbedingungen der verschiedenen Plattformen wie Facebook, Instagram, Twitter, YouTube, TikTok etc. finden auch über den Berichtszeitraum hinaus weitere Prüfungen etwa zur Frage der Erforderlichkeit des Abschlusses von Joint Controller Verträgen statt. In diesem Zuge wurde im Jahr 2021 auch eine Überarbeitung der „Leitlinien zum Datenschutz in den Telemedien und Social Media Angeboten der Rundfunkanstalten“ angestoßen. Die aktualisierte Version wird Anfang 2022 zur Verfügung stehen. Auch die Gremien des öffentlichen Rundfunks haben die zunehmende Bedeutung datenschutzrechtlicher Belange im Bereich der Telemedien erkannt und sich im Zuge der aktuell stattfindenden Prüfung der Telemedienänderungskonzepte mit diesen Themen befasst und entsprechende Fragen an die Geschäftsleitung gestellt.

Was die anonymisierte Nutzungsmessung auf den Angeboten des Hessischen Rundfunks angeht, so wurden, beschleunigt durch das BGH-Urteil vom 28.05.2020 und die Beratungen zum TTDSG, von den Dienstleistern neue Messmethoden vorgestellt, die z.B. ohne das Setzen von Cookies auskommen. Hier werden die weiteren Entwicklungen genau beobachtet.

3.1.3 Cloud-Computing

Aus technischen und wirtschaftlichen Gründen setzt die IT des Hessischen Rundfunks für verschiedene Workflows zunehmend auch auf Cloud-Dienste. Die Geschäftsleitung hat eine entsprechende Cloud-Strategie beschlossen und ein Cloud-Management-Board mit der Steuerung beauftragt. Die Datenschutzbeauftragten haben dabei schon frühzeitig eingefordert, die datenschutzrechtlichen Belange bei der Nutzung solcher Dienste zu berücksichtigen. Dies wurde auch im Weiteren immer wieder angemahnt. So wurde etwa das Cloud-Management-Board bei der Erstellung eines kurzen Leitfadens unterstützt, der sich an Mitarbeitende der IT richtet, die mit der Einführung neuer Dienste betraut sind. Der Leitfaden soll dabei helfen, die wichtigsten Punkte, wie Art und Umfang der verarbeiteten Daten, Standorte der Datenverarbeitung, Sitz des Dienstleisters, Bereitschaft zum Abschluss von Auftragsverarbeitungsverträgen, ggf. unter Einbeziehung von EU-Standardvertragsklauseln etc., vorzuprüfen. So soll die Sensibilität bei den Mitarbeitenden erhöht und datenschutzrechtliche Anforderungen bereits bei der Auswahl der Dienste berücksichtigt werden. Damit will man vermeiden, dass Dienste eingesetzt werden bzw. in die engere Wahl gelangen, die einer Prüfung durch die Datenschutzbeauftragten nicht Stand halten. Die ersten Rückmeldungen aus der IT zum Leitfaden führten erwartungsgemäß zu

komplexen Fragestellungen, die insbesondere durch die EUGH Rechtsprechung zum Privacy Shield nicht einfach zu lösen sind. Es zeigt sich, dass das Thema Drittanbieter-Management einer hohen Aufmerksamkeit bedarf.

3.1.4 Drittanbieter/Datentransfer in Drittländer

Zum Thema Drittanbieter gab es in Abständen konkrete Unterweisungen an Mitarbeitende in verschiedenen Bereichen, schwerpunktmäßig in der IT, Multimedia, ARD-Sternpunkt. Es ist festzustellen, dass die Sensibilität hinsichtlich des Bedarfs zum Abschluss von Auftragsverarbeitungsverträgen erkennbar gesteigert werden konnte. In der IT wird inzwischen ein System zur Abbildung der IT-Architektur genutzt, um dort auch Angaben zu den Dienstleistern zu hinterlegen, wie z.B. Sitz des Unternehmens, Standorte der Datenverarbeitung, Auftragsverarbeitungsvertrag liegt vor/ist abzuschließen etc..

Was das Thema Datentransfer in Drittländer angeht, so wurden der Geschäftsleitung seitens der Datenschutzbeauftragten schriftliche Hinweise zu den Kernaussagen des EuGH-Urteils vom 16.07.2020 übermittelt. Es wurde insbesondere eine Inventur der bestehenden Verhältnisse mit Dienstleistern angestoßen, um einen Überblick über möglicherweise problematische Auftragsverhältnisse zu erlangen. Dabei wurde festgestellt, dass zum Zeitpunkt der Überprüfung größere Datentransfers in Drittländer in der Regel nicht stattfinden (zum Thema Office/Microsoft 365 siehr Kapitel 3.1.9 dieses Berichts). Allerdings lässt sich bei einigen Systemen im Supportfall der Drittlandsbezug nicht gänzlich vermeiden, da zahlreiche Hersteller von Spezialanwendungen z.B. in den USA sitzen. Es gab und gibt daher auch weiterhin regelmäßig Anfragen aus den Fachbereichen in Bezug auf bestehende und abzuschließende Verträge mit Dritten. Die seit dem 04.06.2021 geltenden EU-Standardvertragsklauseln wurden den Fachbereichen mit einigen Erläuterungen zur Verfügung gestellt und in konkreten Einzelfällen wurde gemeinsam mit den Datenschutzbeauftragten über ergänzende technische und organisatorische Maßnahmen beraten. Dabei wird u.a. darauf geachtet, dass sich Back-up Systeme zur Speicherung von Daten in der EU befinden, dass dort, wo es technisch möglich ist, Verschlüsselungsmechanismen angewendet werden und dass Administratoren dafür sensibilisiert werden, beim Erstellen von Tickets im Supportfall nur die Logfiles zu übermitteln, die für die Fehlerbehebung erforderlich sind.

Insgesamt ist festzustellen, dass hierdurch sowohl in den Fachbereichen als auch bei den Datenschutzbeauftragten ein sehr hoher Aufwand bei der Prüfung und Beratung entsteht. Denn in der Regel sind mehrere Abstimmungsrunden mit den Dienstleistern erforderlich, die in den meisten Fällen zwar durchaus bemüht sind, den Regelungen der DSGVO nachzukommen, zumal auch in den sogenannten Drittländern zunehmend strikte Datenschutzgesetze eingeführt worden sind. Gleichwohl ist zu erkennen, dass das Verständnis für Detailfragen bei näherer Betrachtung nicht immer vorhanden und für beide Seiten zufriedenstellend lösbar ist. Dies betrifft z.B. die Einordnung von vermeintlich technischen Daten, wie IP-Adresse und weiteren sogenannten Telemetriedaten[8] als personenbezogene Daten und damit verbunden die Frage, inwieweit Dienstleister diese Daten auch für eigene Zwecke, z.B. der Sicherheit deren Systeme nutzen dürfen.

Die Bearbeitung solcher Detailfragen ist mit den vorhandenen sehr knappen Kapazitäten in Datenschutz und Justitiariat nur nach und nach lösbar, was in den Fachbereichen zwar meistens auf grundsätzliches Verständnis stößt, aber auch dort zu erheblichem Aufwand und Schwierigkeiten bei der Einführung neuer Dienste führt. Dies ist misslich, da es den Datenschutzbeauftragten ein wichtiges Anliegen ist, den Mitarbeitenden des Hessischen Rundfunks ein grundsätzlich positives Bild der datenschutzrechtlichen Belange und den darin liegenden Chancen z.B. für Datensicherheit und verbesserte Transparenz für die Mitarbeiter*inen und Nutzer*innen der Angebote des Hessischen Rundfunks zu vermitteln. Im Bereich des Datentransfers ist dies selbst für juristisch geschulte Fachleute derzeit schwierig.

3.1.5 Einrichtung eines zentralen Servicedesk‘

Im Rahmen der ARD-Strukturreform wurde das ARD-Projekt „Einführung eines zentralen IT-Service-Desks (zsD) für ARD, ZDF, DLR“ initiiert, an dem auch der hr beteiligt ist.

Unter einer einheitlichen, zentralen Telefonnummer und/oder E-Mail-Adresse können sich alle hr-Mitarbeitenden (und die Mitarbeitenden der anderen beteiligten Rundfunkanstalten) an diesen Servicedesk wenden, sofern sie Hilfestellung bei IT-spezifischen Fragestellungen bezüglich Software und/oder Hardware benötigen.

[8] Telemetriedaten: Dabei handet es sich um Diagnose- und Funktionsdaten, die per Fernzugriff von einem Dienstleister zur Steuerung seiner Produktentwicklung, Produktsicherheit etc. bei der Nutzung seiner Dienste gesammelt werden. Auch wenn es sich meist um technische Informationen handelt, weisen zumindest einige dieser Daten einen Personenbezug zu den Nutzer*innen nach DSGVO auf.

Durch die Einführung dieses zentralen Servicedesks sollte erreicht werden, dass der sogenannte „first level support“ *zentral* für *alle* beteiligten Rundfunkanstalten erbracht werden kann, ohne dass jede Rundfunkanstalt für sich die hierfür jeweils erforderlichen Mitarbeiterkapazitäten vorhalten müsste.

Bei der Umsetzung dieses Vorhabens zeigte sich – so wie das heutzutage oftmals üblich ist – dass zur Realisierung des Projekts die Einbindung gleich mehrerer Dienstleister erforderlich war. Der eine Dienstleister fungiert als „Generalunternehmer“ und stellt die räumliche, technische und personelle Infrastruktur für den „first level support“ bereit. Die für die Erbringung dieser Dienstleistung erforderliche Software (Ticketing-System) wird wiederum von einem anderen Dienstleister zur Verfügung gestellt und schließlich wird diese Software in einem separaten Rechenzentrum gehostet, das von einem weiteren Dienstleister betrieben wird.

Dadurch sind gleich mehrere Dienstleister involviert, die ihrerseits gegebenenfalls Unter-Auftragnehmer beauftragten und dadurch die Zahl der insgesamt eingesetzten Dienstleister „beliebig“ zunehmen kann.

Da es auch in solchen Fällen um die Verarbeitung von personenbezogenen Daten geht, und der hr letztendlich im datenschutzrechtlichen Sinne als „Verantwortlicher“ gemäß Artikel 4 Nr. 7. DSGVO anzusehen ist, müssen nicht nur die Dienstleister (und ggf. die entsprechenden Unter-Auftragnehmer) sorgfältig ausgewählt werden, sondern es müssen auch andere, teilweise aufwändig zu prüfende datenschutzrechtliche Anforderungen berücksichtig und erfüllt werden.

So wurde beispielsweise eine „Schutzbedarfsfeststellung“ durchgeführt, mit der der Schutzbedarf der verarbeiteten Daten im Hinblick auf die Kriterien „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ ermittelt wird. Im Fall des zentralen Servicedesk‘ wurde dieser Schutzbedarf als „normal“ eingestuft. In der abschließenden Beurteilung wurde ein „sehr hohes Maß der Sicherheitsmaßnahmen“ attestiert.

Im Rahmen des Projekts wurde außerdem eine sogenannte „Datenschutzfolgenabschätzung (DSFA)“ gemäß Artikel 35 DSGVO vorgenommen. Eine solche DSFA ist dann durchzuführen, wenn sich durch die Verarbeitung der personenbezogenen Daten *„ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen*“ ergeben kann.

Letztlich geht es darum, durch eine derartige DSFA die aus der Verarbeitung der personenbezogenen Daten ggf. resultierenden Risiken für die Betroffenen zu identifizieren, diese zu bewerten und ggf. Maßnahmen zu ergreifen bzw. zu beschreiben, die der Risikominimierung dienen. Im Ergebnis der

Betrachtung wurde für die Verarbeitung personenbezogener Daten im Rahmen des zentralen Servicedesk jedoch kein solches hohes Risiko identifiziert.

Schließlich wurde den *formalen* datenschutzrechtlichen Anforderungen durch den Abschluss mehrerer „Vereinbarungen zur Auftragsverarbeitung" gemäß Artikel 28 DSGVO mit den jeweiligen Dienstleistern entsprochen.

3.1.6 Einrichtung einer zentrale Endgeräte-Datenbank

Im Rahmen der Einführung des zentralen Servicedesks (zSD) sollte auch eine zentrale Endgeräte-Datenbank installiert werden, damit die im zentralen Servicedesk tätigen Mitarbeiter*innen auf die Daten und die Historie der entsprechenden Endgeräte zugreifen können.

Das hierbei zum Einsatz kommende Programm verfügt über diverse Schnittstellen zu bereits existierenden IT-Systemen des Hessischen Rundfunk und wird aus diesen Systemen heraus mit entsprechenden Daten „befüllt".

Hier waren die datenschutzrechtlichen Anforderungen relativ leicht zu erfüllen.

Zum einen werden mit dieser Anwendung lediglich wenige personenbezogene Daten verarbeitet. Zum anderen handelt es sich um eine Anwendung, die auf Servern des Hessischen Rundfunks installiert ist („on premises-Lösung") und damit die Verarbeitung der personenbezogenen Daten den vom Hessischen Rundfunk selbst implementierten technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit unterfällt. Durch ein entsprechendes Berechtigungs- und Rollenkonzept ist darüber hinaus sichergestellt, dass lediglich berechtigte Nutzer*innen auf die Anwendung zugreifen können.

Die Nutzer*innen des Systems haben außerdem jeweils entsprechende Vertraulichkeitserklärungen unterzeichnet. Da es sich wie unter dem Punkt „zentraler Servicedesk" dargestellt um externe Mitarbeiter*innen eines Dienstleisters handelt, wurde auch hier eine „Vereinbarung zur Auftragsverarbeitung" geschlossen.

Daher waren auch bei diesem Projekt sämtliche datenschutzrechtlich relevanten Sachverhalte berücksichtigt und die entsprechenden Anforderungen erfüllt.

3.1.7 Etablierung einer Cloud-Security Plattform

Zur Steuerung des Internetverkehrs wird beim hr – wie bei anderen Rundfunkanstalten und in der Industrie auch – eine „Web-Proxy-Lösung“ eingesetzt.

Hierbei ist ein sogenannter „Proxy-Server“ zwischen den einzelnen clients (PCs der Mitarbeiter*innen) und „dem Internet“ angeordnet. Er „filtert“ in gewisser Weise den Verbindungsaufbau mit dem Internet, indem beispielsweise bestimmte „Regeln“ und „Zugriffsberechtigungen“ hinterlegt und dann automatisch ausgeführt werden können.

Das vom Hessischen Rundfunk bisher eingesetzte Produkt wurde aus unterschiedlichen Gründen durch ein neues, wirtschaftlicheres und zukunftsfähigeres System abgelöst. Dieses System ist außerdem besser als das bisherige geeignet, die sich in Zeiten der „Corona-Pandemie“ aus dem „mobilen Arbeiten“ ergebenden Anforderungen zu erfüllen.

Zum Einsatz eines solchen Produkts ist der Hessische Rundfunk quasi „angehalten“, da er gemäß Artikel 24 DSGVO i.V.m. Artikel 32 DSGVO verpflichtet ist, geeignete technische und organisatorische Maßnahmen umzusetzen, um die Einhaltung der DSGVO-Vorschriften sicherzustellen. Hierzu gehört auch, die Sicherheit der Datenverarbeitung durch entsprechende Maßnahmen, z.B. den Einsatz eines derartigen Produkts zu gewährleisten.

Allerdings handelt es sich bei dem neuen Produkt um ein amerikanisches, cloud-basiertes Produkt. Da auch hier (in geringem Umfang) personenbezogene Daten verarbeitet werden, und es sich bei den USA im datenschutzrechtlichen Sinne um ein sogenanntes „Drittland“ handelt, müssen die sich aus Artikel 44 ff. DSGVO ergebenden Anforderungen geprüft und erfüllt werden.

Der Anbieter ist als sogenannter „Auftragsverarbeiter“ anzusehen und darf insoweit die Verarbeitung personenbezogener Daten nur auf Weisung des hr vornehmen. Daher war es auch hier erforderlich, mit dem Anbieter eine entsprechende „Vereinbarung zur Auftragsverarbeitung“ abzuschließen. Hierbei wurden die „EU-Standardvertragsklauseln“ integriert, um den genannten Anforderungen der Artikel 44 ff. DSGO gerecht zu werden.

Außerdem wurde festgelegt, dass insgesamt nur wenige personenbezogene Daten verarbeitet werden, die Verarbeitung dieser Daten ausschließlich in europäischen Rechenzentren erfolgt und sämtliche Daten nach spätestens sechs Monaten gelöscht werden müssen.

Da damit die aus Sicht des Datenschutzes wesentlichen Anforderungen erfüllt waren, konnte auch diesem Vorhaben zugestimmt werden.

3.1.8 Neuer Virenscanner

Auch der bisher vom Hessischen Rundfunk zum Schutz vor diverser Schadsoftware eingesetzte Virenscanner musste abgelöst werden, da das Produkt als „veraltet“ galt, die Lizenzen ausliefen und eine neue Lösung einen aktuelleren und größeren Funktionsumfang bieten sollte.

Nachdem eine interne Projektgruppe eine Markterkundung durchgeführt und die Vor- und Nachteile der einzelnen Produkte gegeneinander abgewogen hatte, fiel die Entscheidung – erneut – auf das Produkt eines US-amerikanischen Anbieters, das als Standard Endpoint-Security-Lösung zum Einsatz kommt.

Das Produkt dient dem Schutz vor Malware und soll die Client- und Serversysteme des Hessischen Rundfunks vor Schadcode schützen. Dazu werden die IT-Systemprozesse der Client- und Server-Infrastruktur des Hessischen Rundfunks durch dieses Produkt „überwacht“ und die hieraus resultierenden Erkenntnisse werden mit Hilfe „maschinellen Lernens des Systems“ kombiniert, um so (potenziell) gefährliche Verhaltensweisen der IT-System identifizieren zu können und damit die IT-Infrastruktur des Hessischen Rundfunks vor aktuellen und gezielten Bedrohungen zu schützen.

Wie bereits unter Punkt 3.1.7 ausgeführt, ist der Hessische Rundfunk gemäß Artikel 24 DSGVO i.V.m. Artikel 32 DSGVO verpflichtet, geeignete technische und organisatorische Maßnahmen umzusetzen, um die Einhaltung der DSGVO-Vorschriften sicherzustellen. Hierzu gehört u.a. auch, die Sicherheit der Datenverarbeitung durch das Ergreifen entsprechender Maßnahmen, z.B. den Einsatz eines entsprechenden Virenscanners zu gewährleisten.

Darüber hinaus musste auch hier eine „Vereinbarung zur Auftragsverarbeitung“ (unter Einschluss der „EU-Standardvertragsklauseln“) abgeschlossen sowie eine „Schutzbedarfsfeststellung“ durchgeführt werden.

Auch der geographische Ort, an dem die Datenverarbeitung erfolgen darf, wurde eingeschränkt; die entsprechenden Rechenzentren befinden sich in Frankfurt am Main und sind bezüglich der Einhaltung von Standards der Datensicherheit zertifiziert (ISO 27001, SOC 2[9]). Sämtliche verarbeiteten Daten werden verschlüsselt. Auch wenn es sich mehrheitlich um technische Daten handelt, werden hier in geringem Umfang ebenfalls personenbezogene Daten verarbeitet. Die unterschiedlichen Daten verlassen jedoch nicht den Geltungsbereich der DSGVO. Datentransfers in die USA werden durch entsprechende technische Einstellungen des Hessischen Rundfunks unterbunden.

[9] „SOC“ = Service Organization Control ; „IT-Sicherheitsstandard“, der die Kriterien ‚Sicherheit‘, ‚Verfügbarkeit‘, ‚Integrität‘, ‚Vertraulichkeit‘ und ‚Datenschutz‘ umfasst

Trotz relativ frühzeitiger Einbindung meiner Person kam es – wie in derartigen Fällen (Cloud-Anbieter mit Sitz in den USA) leider üblich – zu zeitlichen Verzögerungen, die letztendlich darauf zurückzuführen waren, dass die im Rahmen einer derartigen Auftragsverarbeitung aus datenschutzrechtlicher Sicht vertraglich zu fixierenden Sachverhalte mit dem (US-amerikanischen) Auftragnehmer geklärt und schriftlich festgelegt werden müssen. Dieser Abstimmungsprozess verursacht erfahrungsgemäß auf beiden Seiten nicht unerhebliche Aufwände, so dass sich der gesamte Prozess ziemlich aufwändig gestaltet.

Letztendlich konnten die Verhandlungen jedoch auch hier zu einem erfolgreichen Ende gebracht werden.

3.1.9 Einführung Microsoft 365

Erklärtes Ziel des im Hessischen Rundfunks laufenden Strategieprozesses ist es, den Hessischen Rundfunk weg von einem „linearen Sender“ hin zu einem „digitalen Medienunternehmen“ zu entwickeln.

Hierzu sollen die Arbeitsprozesse digitalisiert, die elektronischen Kommunikations- und Arbeitsmittel enger miteinander verzahnt und so eine effizientere, kollaborative Arbeitsweise ermöglicht werden. Zur Umsetzung müssen entsprechende Anwendungen installiert werden.

Daher wurde bereits im Mai 2019 eine Projektgruppe beauftragt, die Rahmenbedingungen für die Einführung des Produkts „Microsoft 365“ zu klären.

Die Wahl fiel auf „Microsoft 365“, da die unterschiedlichen Microsoft-Anwendungen bereits in vielfältiger Weise beim Hessischen Rundfunk eingesetzt werden, damit einen „quasi-Standard“ darstellen und somit der Umstieg auf eine „komplett neue Basis“ (z.B. Open Source) aus wirtschaftlichen Gründen nicht realisierbar war.

Bei „Microsoft 365“ handelt es sich „natürlich“ um ein weiteres Produkt, das als Cloud-Anwendung vertrieben wird. Die meisten großen Software-Hersteller (Microsoft, SAP, Adobe etc.) sind seit einiger Zeit dazu übergegangen, ihre Anwendungen nicht mehr als klassisches Software-Paket anzubieten, bei dem der Käufer in der Lage ist, die Software auf seinen eigenen Servern zu installieren und damit die „Datenhoheit“ im eigenen Verfügungs- und Verantwortungsbereich zu halten. Vielmehr werden die Anwendungen „in der Cloud“ bereitgestellt (sogenanntes „Software as a Service-Modell“ – SaaS) und der Kunde erwirbt lediglich entsprechende, zeitlich befristete, Lizenzen um die Software nutzen zu können. Durch die Auslagerung auf den Anbieter ergeben sich natürlich u.a. Fragen des Datenschutzes, die auch im Rahmen dieses Projekts geklärt werden mussten.

Bei Microsoft handelt es sich um einen US-amerikanischen Anbieter, der als solcher der US-amerikanischen Gesetzgebung unterliegt, die im Hinblick auf den Datenschutz gemäß höchstrichterlicher Rechtsprechung (EuGH) nicht dem europäischen Standard entspricht. Die USA werden in diesem Zusammenhang als sogenanntes (datenschutzrechtlich unsicheres) „Drittland" betrachtet, in dem die datenschutzrechtlichen Regelungen der DSGVO nicht oder nur in eingeschränktem Umfang Gültigkeit besitzen.

Insoweit ist es erforderlich, den Einsatz des Produkts besonders sorgfältig zu prüfen und gegebenenfalls zusätzliche Maßnahmen zu ergreifen, um eine adäquate Sicherheit der Datenverarbeitung gleichwohl gewährleisten zu können.

Diese adäquate Sicherheit der Datenverarbeitung wurde beim Einsatz von „Microsoft 365" u.a. durch folgende Maßnahmen sichergestellt:

- Die abgeschlossenen vertraglichen Regelungen (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) beinhalten im Hinblick auf den Datenschutz u.a. auch die „EU-Standardvertragsklauseln"; darüber hinaus wurden „zusätzliche Garantien" vereinbart, z.B. dergestalt, dass Microsoft zusichert, dem Hessischen Rundfunk mitzuteilen, wenn US-Sicherheitsbehörden einen entsprechenden Zugriff auf die Daten des Hessischen Rundfunks fordern,
- Die Übermittlung der sogenannten „Telemetriedaten"[10] wird technisch weitgehend unterbunden,
- Die übrigen (personenbezogenen)Daten werden in europäischen Rechenzentren von Microsoft verarbeitet, so dass hier die Regelungen der DSGVO Geltung entfalten können,
- Um die mit dem Einsatz der Anwendung verbundenen Risiken für die Nutzer*innen des Systems zu bewerten, wurde nicht nur eine interne IT-Risikoanalyse durchgeführt, sondern erneut auch eine sogenannte „Datenschutzfolgenabschätzung" (DSFA) gemäß Artikel 35 DSGVO vorgenommen. Die in diesem Zusammenhang sich ergebenden Risiken wurden identifiziert, bewertet und – soweit erforderlich – entsprechende risikoausschließende oder zumindest -minimierende Maßnahmen beschlossen und umgesetzt
- Schließlich wurde zwischen Geschäftsleitung und Gesamtpersonalrat eine Rahmen-Dienstvereinbarung abgeschlossen, die die

[10] Diese „Telemetriedaten" umfassen beispielsweise Sachverhalte wie „Versionsangaben", „Nutzungsverhalten" und „Absturzberichte", die von Microsoft zu eigenen Zwecken verarbeitet werden.

Rahmenbedingungen des Einsatzes von „Microsoft 365“ regelt und dem Interessenausgleich zwischen dem Hessischen Rundfunk einerseits und den Beschäftigten andererseits dient.

Trotz der Umsetzung entsprechender Maßnahmen ist es u.a. aufgrund der sich ständig ändernden Gegebenheiten auf Seiten Microsoft notwendig, die vorgenannte „IT-Risikoanalyse“ und „Datenschutzfolgenabschätzung“ künftig in regelmäßigen Abständen durchzuführen, um diese fortlaufend an die neuen Gegebenheiten und Erkenntnisse anpassen zu können.

3.2 Datenschutz im Programm- und Produktionsbereich

NAnU (Neue Anlage für Untertitelsystem)

Um blinden, gehörlosen oder schwerhörigen Kund*innen die Nutzung der vielfältigen Angebote im Fernsehen sowie beim Internet-Auftritt des Hessischen Rundfunks zu erleichtern bzw. erst zu ermöglichen, müssen die barrierefreien Angebote im Hessischen Rundfunk ständig aktualisiert und ausgebaut werden.

Die bisher für Zwecke der Untertitelung eingesetzte spezielle Software war veraltet und wurde herstellerseitig nicht mehr unterstützt, so dass sie durch ein neues Produkt ersetzt werden musste.

Beim Einsatz einer solchen Software werden auch personenbezogene Daten verarbeitet. Insoweit sind auch hier die einschlägigen datenschutzrechtlichen Regelungen zu berücksichtigen.

Generell dient die für die Untertitelung eingesetzte Software der Herstellung eines journalistischen Produkts. Insoweit unterfällt die Verarbeitung der personenbezogenen Daten insgesamt dem sogenannten „Medienprivileg“. Dies bedeutet, dass nur relativ wenige der in der DSGVO existierenden datenschutzrechtlichen Vorschriften Berücksichtigung finden müssen und im Wesentlichen die Sicherheit der Datenverarbeitung zu gewährleisten ist.

Da es sich bei der eingesetzten Software – entgegen dem üblichen Trend! – *nicht* um eine „Cloud-Lösung“ handelt, konnte die Sicherheit der Datenverarbeitung dadurch gewährleistet werden, dass der Hessische Rundfunk die Software käuflich erworben und auf seinen eigenen Servern und PC-Clients installiert hat.

Da die Wartung der Software von externen Dienstleistern zum Teil über Fernwartung durchgeführt wird, kann eine Kenntnisnahme personenbezogener Daten (des Hessischen Rundfunks) im Rahmen dieser Wartungstätigkeit nicht ausgeschlossen werden. Daher musste zwischen dem Hessischen

Rundfunk und dem Dienstleister noch schriftlich eine datenschutzrechtlich erforderliche Vereinbarung zur Auftragsverarbeitung abgeschlossen werden und somit war auch aus Sicht des Datenschutzes die Implementierung dieser Software zulässig.

E-learning-Plattform für die Fort- und Weiterbildung

Die ständige Aus- und Fortbildung der Mitarbeiter*innen des Hessischen Rundfunks dient der kontinuierlichen (Weiter-)Qualifizierung der Mitarbeiter*innen und stellt in gewissem Maße auch die Wettbewerbsfähigkeit des Hessischen Rundfunks sicher.

Um den Anforderungen an die neuen Arbeitswelten sowie den geänderten Erwartungen der Mitarbeiter*innen im Hinblick auf Fortbildungsangebote gerecht werden zu können, sollen neben den klassischen Präsenzveranstaltungen – zumal in Zeiten des „Corona-Virus'" - auch sogenannte E-learning-Plattformen bzw. „interaktive Lernplattformen" angeboten werden. Im Rahmen derartiger Aus- und Fortbildungsmaßnahmen durchlaufen die jeweiligen Mitarbeiter*innen ein „online-tutorial" im Selbststudium. Damit ist ein orts- und zeitunabhängiges Lernen bzw. eine entsprechende (Weiter-)Qualifizierung möglich.

Die ARD.ZDF medienakademie („mak")[11] hat hierfür ein „Lernmanagement-System" entwickelt und stellt diese Plattform den beteiligten Rundfunkanstalten zur Verfügung.

Im Rahmen der Nutzung dieses Systems durch die Mitarbeiter*innen des Hessischen Rundfunks werden natürlich auch deren personenbezogene Daten verarbeitet. Daher waren auch hier datenschutzrechtliche Anforderungen zu prüfen.

Die Verarbeitung der personenbezogenen Daten wird in diesem Fall eigenverantwortlich von der „mak" vorgenommen, diese gilt als „Verantwortlicher" im Sinne von Artikel 4 Nr. 7. DSGVO.

Dies bedeutet u.a., dass die aus Sicht des Datenschutzes und der Daten- bzw. IT-Sicherheit erforderlichen Dokumentationen wie beispielsweise das „Verzeichnis von Verarbeitungstätigkeiten" oder auch die Erarbeitung von Rollen- und Berechtigungskonzepten in der Verantwortung der „mak" liegen. Die entsprechenden Dokumente wurden den beteiligten Rundfunkanstalten, so auch dem hr, allerdings zur Prüfung zur Verfügung gestellt..

[11] Die Gesellschafter der ARD.ZDF medienakademie sind die Rundfunkanstalten der ARD, das ZDF und das Deutschlandradio. Die „mak" bietet offene Seminare u.a. als E-learning und Inhouse-Trainings an

Weitere Punkte, die die Einhaltung der Datenschutz-Vorgaben gewährleisten, sind z.B.:

- Die Verarbeitung der entsprechenden personenbezogenen Daten erfolgt auf Basis einer transparenten und informierten Einwilligung der Nutzer*innen (Artikel 6 Abs. 1 lit. a) DSGVO),
- bei der Entwicklung der Lernplattform wurde darauf geachtet, dass nur diejenigen personenbezogenen Daten erfasst und verarbeitet werden, die zum Betreiben der Plattform erforderlich sind („Datenminmierung“ bzw. “Datensparsamkeit“ gemäß Artikel 5 Abs. 1 lit. c) DSGVO),
- die im Rahmen der Verarbeitung anfallenden personenbezogenen Daten werden nur für den Zweck der Vermittlung entsprechender Lerninhalte verwendet. Eine Weitergabe an Dritte oder eine Leistungs- und Verhaltenskontrolle findet nicht statt,
- durch ein rollenbasiertes Berechtigungskonzept ist sichergestellt, dass lediglich berechtige Personen auf entsprechende Informationen zugreifen können,
- die das System betreuenden Personen (Administratoren) sowie Personen, die über umfängliche Systemrechte verfügen, müssen eine entsprechende Datenschutz- und Vertraulichkeitserklärung unterzeichnen.
- die Transparenz bei der Datenverarbeitung wird dadurch sichergestellt, dass die Nutzer*innen bei der Erstanmeldung am System über die „Nutzungsbedingungen und Datenschutzerklärung“ der Lernplattform informiert werden und diese akzeptieren müssen.

Auch hier konnte daher die datenschutzrechtliche Zustimmung zur Inbetriebnahme erteilt werden.

Adobe CC „Creative Cloud“

Wie bereits mehrfach erwähnt, werden auch beim Hessischen Rundfunk zunehmend Produkte eingesetzt, die „in der Cloud“ bereitgestellt werden.

Dieser Trend setzt sich auch fort beim Einsatz einer Software für die Fotobearbeitung bzw. das Grafikdesign und die Webentwicklung. Mithilfe derartiger Programme werden z.B. grafische Inhalte für das Internet und die Social-Media-Kanäle des Hessischen Rundfunks erstellt.

Obwohl solche Programme bereits seit vielen Jahren eingesetzt werden, musste auch in diesem Fall auf die cloud-basierte Anwendung des Anbieters umgestiegen werden.

Dementsprechend wurde auch hier die erforderliche Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO unter Einschluss der EU-Standardvertragsklauseln abgeschlossen. Darin wird zum einen schriftlich vereinbart, dass die Verarbeitung personenbezogener Daten beim Anbieter nur auf Weisung der Rundfunkanstalten erfolgen darf. Zum anderen wird vom Anbieter die Einhaltung sogenannter technisch-organisatorischer Maßnahmen vertraglich zugesichert, damit die Sicherheit der Datenverarbeitung gewährleistet werden kann.

Darüber hinaus müssen in solchen Fällen interne Regelungen und Anweisungen getroffen werden, die festlegen, welche (personenbezogenen)Daten und Inhalte „in der Cloud" verarbeitet werden dürfen und welche Daten – z.B. im Fall einer investigativen Recherche – besser nicht in den weltweiten Rechenzentren der Cloud abgelegt werden.

Da insgesamt jedoch nur sehr wenige personenbezogen Daten von der Anwendung verarbeitet werden, konnte der Einführung und Nutzung des Produkt aus Sicht des Datenschutzes auch in diesem Fall zugestimmt werden.

ARD-Jugendmedientag 2020

Gemeinsam mit anderen ARD-Rundfunkanstalten wurde im November 2020 der „ARD-Jugendmedientag 2020" veranstaltet.

Aufgrund der auch damals schon herrschenden „Corona-Lage" konnte der Jugendmedientag nicht als Präsenzveranstaltung durchgeführt werden, sondern musste ausschließlich online stattfinden.

Für den Jugendmedientages waren ca. 100 Web-Workshops geplant. An diesen Workshops sollten sich – dem Konzept des Jugendmedientages entsprechend – diverse Schulen und Schüler*innen beteiligen. Da hier eine einheitliche Nutzung des beim Hessischen Rundfunks eingesetzten Programms „Microsoft Teams" nicht möglich war, musste eine andere, für alle Teilnehmer*innen einheitliche und datenschutzkonforme Videokonferenz-Plattform gefunden werden.

Letztendlich hat man sich für das Tool „BigBlueButton" entschieden, u.a. deswegen, weil es sich um ein einfach zu bedienendes und sehr sicheres Tool handelt. Außerdem wird dieses Tool schon lange vom Kooperationspartner des Hessischen Rundfunks (Hessisches Kultusministerium) genutzt.

„BigBlueButton" wurde jedoch vom Hessischen Rundfunk nicht direkt genutzt. Vielmehr war eine Agentur zwischengeschaltet, die auch die gesamte Organisation der Veranstaltung übernommen hat.

Mit dieser Agentur musste eine Vereinbarung zur Auftragsverarbeitung geschlossen werden, die Bedingungen des Anbieters mussten geprüft und die getroffenen technisch-organisatorischen Maßnahmen beurteilt werden.

Nachdem sichergestellt war, dass die Verarbeitung der personenbezogenen Daten ausschließlich in einem deutschen Rechenzentrum erfolgt, die Teilnehmer*innen in transparenter Art und Weise über die Datenverarbeitung aufgeklärt wurden und in diese einwilligen mussten und außerdem festgelegt wurde, dass keine Aufzeichnung der Veranstaltung erfolgte, konnte auch diesem Vorhaben aus datenschutzrechtlicher Sicht zugestimmt werden.

Software für Sprachaufnahmen/Audioproduktionen über Internet

Aufgrund der Corona-Pandemie konnten keine oder zumindest nur möglichst wenige externe Gäste das Gelände des Hessischen Rundfunks betreten.

Hiervon betroffen waren beispielsweise auch Studiogäste für Hörfunksendungen oder Sprecher*innen für die Synchronisation von Fernsehproduktionen.

Aus diesem Grund wurde geprüft, mit welchen Diensten eine Zuschaltung Externer mit einer sehr guten Audioqualität und gleichzeitig geringem Aufwand für den zugeschalteten Gast möglich ist. Als ein entsprechendes Produkt gefunden war, mussten natürlich auch die datenschutzrechtlichen Anforderungen erfüllt werden.

Das eingesetzte Produkt stellt hochwertige Audioverbindungen über das Internet mit einem möglichst einfachen Verfahren für die Anwender*innen bereit.

Dabei ist das gesamte Verfahren sowohl für die externen Gäste als auch die Mitarbeiter*innen des Hessischen Rundfunks transparent und einfach gestaltet.

Die externen Gäste erhalten per E-Mail einen entsprechenden link, mit dessen Hilfe eine Einwahl in das System möglich ist. Dabei müssen die externen Gäste keinerlei persönliche, personenbezogene Daten eingeben. Außerdem muss auf dem Gerät der jeweiligen Nutzer*in keine spezielle Software installiert werden.

Die Mitarbeiter*innen des Hessischen Rundfunks müssen ebenfalls keine personenbezogenen Daten preisgeben, da die Arbeit mit dem System über sogenannte Funktionsaccounts erfolgt, denen keine bestimmte Person

zugeordnet ist. Außerdem wurde der Kreis der Berechtigten, die mit dem System arbeiten dürfen, sehr klein gehalten.

Darüber hinaus erfolgt die Verarbeitung der Daten in europäischen Rechenzentren, so dass die Regelungen der DSGVO vollumfänglich Gültigkeit besitzen. Außerdem werden die für die Erstellung entsprechender Kundenkonten notwendigen Kundendaten verschlüsselt gespeichert.

4. Datenschutz beim Rundfunkbeitrag

Zum 1. Januar 2013 wurde die ehemalige Gebühreneinzugszentrale (GEZ) in „ARD, ZDF, Deutschlandradio Beitragsservice“ (zentraler Beitragsservice) umbenannt.

Der im Juli 2020 veröffentlichte Geschäftsbericht des Beitragsservice für das Jahr 2019 weist rund 46 Millionen Beitragskonten, bestehend aus ca. 39,7 Millionen Wohnungen, rund 4,0 Millionen Betriebsstätten, ca. 1,1 Millionen Gästezimmer und Ferienwohnungen sowie nahezu 4,5 Millionen Kraftfahrzeuge aus.

Der zentrale Beitragsservice in Köln ist das gemeinsame Rechenzentrum der ARD-Landesrundfunkanstalten, des ZDF und Deutschlandradio. Es speichert und verarbeitet die für den Rundfunkbeitrag erforderlichen Beitragszahlerdaten im Auftrag der Landesrundfunkanstalten. Datenschutzrechtlich verantwortlich bleibt die jeweils für ein Gebiet zuständige Rundfunkanstalt, z.B. für die hessischen Beitragszahlerdaten der Hessische Rundfunk. Wenn es um die Verarbeitung der hessischen Beitragszahlerdaten geht, findet demnach das Hessische Datenschutzrecht Anwendung, vorrangig jedoch die bereichsspezifischen Datenschutzregelungen des Rundfunkbeitragsstaatsvertrages (RBStV). Der zentrale Beitragsservice arbeitet datenschutzrechtlich im Auftrag der Landesrundfunkanstalten. Die betriebliche Datenschutzbeauftragte des zentralen Beitragsservice arbeitet mit dem/den nach Landesrecht zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese über Verstöße gegen Datenschutzvorschriften und eingeleitete Maßnahmen.

Aufgrund der im datenschutzrechlichen Sinne „gemeinsamen Verantwortung“ von einerseits den einzelnen Rundfunkanstalten und andererseits dem Zentralen Beitragsservice ist es erforderlich, die hieraus resultierenden datenschutzrechtlichen Verpflichtungen in einer schriftlichen Vereinbarung gemäß Artikel 26 DSGVO zu regeln. Eine solche „Joint-Controller-

Vereinbarung“ liegt zum Zeitpunkt der Erstellung dieses Tätigkeitsberichts in unterschriftsreifer Form vor.

Fragen mit direktem Hessen- bzw. hr-Bezug

Einzelfälle (Anfragen, Beschwerden)

Anfragen und Beschwerden zum Datenschutz beim Rundfunkbeitragseinzug haben in Hessen mehrere mögliche Adressaten:

- Sie werden direkt an den **Datenschutzbeauftragten des Hessischen Rundfunks** gerichtet, dessen Name und Adresse u. a. auf den Internet-Seiten des zentralen Beitragsservice zu finden sind.

- Sie werden an den **zentralen Beitragsservice in Köln** gesandt, deren Datenschutzbeauftragte die Eingaben normalerweise beantwortet und bei eventuellen Rückfragen den Datenschutzbeauftragten der jeweiligen Landesrundfunkanstalt einschaltet.

- Eine unbekannte Anzahl von Fragen und Beschwerden gelangt zum **Hessischen Beauftragten für Datenschutz und Informationsfreiheit**, der diese entweder aus seinem Wissen und der Erfahrung heraus beantwortet und/oder zur Aufklärung des Sachverhaltes den Beitragsservice und/oder den Datenschutzbeauftragten des hr einbezieht.

- Schließlich enthalten die Anfragen und Eingaben zum Rundfunkbeitrag, die direkt an den **Beitragsservice des hr** gesandt werden, oft auch Fragen von datenschutzrechtlicher Relevanz, die mit mir besprochen werden.

Eingaben an den hr-Datenschutzbeauftragten

Wie in meinen vorangegangenen Tätigkeitsberichten dargestellt, handelte es sich in der Vergangenheit bei den an mich gerichteten Eingaben überwiegend um Beschwerden über das Vorgehen und die Tätigkeit der Rundfunkgebührenbeauftragten. Dieser Beauftragtendienst wurde im Zuge der Umstellung auf den Rundfunkbeitrag im Sommer 2013 beim Hessischen Rundfunk eingestellt, so dass mich seitdem keine derartigen Eingaben mehr erreichen.

Mit den meisten an mich gerichteten Eingaben machen die Betroffenen Gebrauch von Ihrem Auskunftsrecht und bitten um Auskunft über die zu ihrer Person gespeicherten Daten. Diese Anfragen werden von mir zuständigkeitshalber an den Beitragsservice des Hessischen Rundfunks mit der Bitte um Beantwortung weitergeleitet.

Eingaben aus Hessen an den zentralen Beitragsservice

Im Jahr 2021 wurden insgesamt 538 Anfragen aus dem Zuständigkeitsbereich des hr vom zentralen Beitragsservice bearbeitet. Hierbei handelte es sich um 534 sogeannte „einfache Datenauskünfte“ (davon 210 elektronisch beantragt) und 4 „erweiterte Datenauskünfte“.

5. Arbeitskreis der Datenschutzbeauftragten ARD/ZDF/ Deutschlandradio (AK DSB)

Die Datenschutzbeauftragten der ARD, des ZDF, des Deutschlandradios und des zentralen Beitragsservice haben sich 1979 zum Arbeitskreis Datenschutzbeauftragte ARD/ZDF (AK DSB) zusammengeschlossen, um regelmäßig Meinungen und Erfahrungen auszutauschen, aber auch um bei ähnlichen Problemen möglichst einheitliche Maßnahmen und Verfahren abzustimmen.

Der AK DSB trifft sich üblicherweise regelmäßig zweimal pro Jahr. Aufgrund der immer noch andauernden sogenannten „Corona-Pandemie“ fanden die Sitzungen im Berichtszeitraum ausschließlich als Videokonferenzen und nicht als Präsenzsitzungen statt. Auch der über die regulären Sitzungen hinausgehende Austausch zu spezifischen Einzelthemen wurde jeweils als Videokonferenz durchgeführt.

Der Vorsitz im AK DSB wechselt im Zwei-Jahres-Rhythmus. Im Berichtszeitraum führte der Rundfunkdatenschutzbeauftragte des NDR, Herr Dr. Heiko Neuhoff den Vorsitz. Bereits in der AK DSB-Sitzung vom 19./20.11.2020 wurde Herr Axel Schneider vom BR als neuer Vorsitzender für die Jahre 2022 und 2023 gewählt. Zum stellvertretenden Vorsitzenden für diesen Zeitraum wurde Herr Gerold Plachky vom ZDF gewählt

Im Rahmen der Sitzungen des AK DSB wurden im Berichtszeitraum insbesondere die folgenden Themen behandelt:

- Entwicklung und Umsetzung der Europäischen Datenschutzgrundverordnung.
- Sicherstellung des Datenschutzes im redaktionellen Bereich.
- Datenschutzrechtliche Anforderungen bei der möglichen Einführung von Cloud-Diensten.

- Vereinheitlichung der Datenschutzfolgenabschätzungen in den einzelnen Rundfunkanstalten
- Überarbeitung der Muster zur Auftragsverarbeitung und des Verzeichnisses von Verarbeitungstätigkeiten
- Weiteres Vorgehen in Sachen EuGH-Urteil zu Facebook-Fanpages
- Verfahren zur Meldung von Datenschutzverletzungen
- Auftragsverarbeitung und Übermittlung in Drittländer
- Begleitung des SAP-Harmonisierungsprozesses innerhalb der Rundfunkanstalten

6. Rundfunkdatenschutzkonferenz (RDSK)

Bereits im April 2019 erfolgte die Gründung der RDSK als Konferenz der unabhängigen Datenschutzaufsichtsbehörden im öffentlich-rechtlichen Rundfunk.

Der öffentlich-rechtliche Rundfunk in Deutschland muss gemäß Artikel 5 Abs. 1 S. 2 GG und der Rechtsprechung des Bundesverfassungsgerichts staatsfern organisiert sein. Er unterliegt deshalb einer autonomen Datenschutzaufsicht, die an die Stelle der staatlichen Datenschutzkontrolle tritt. Hierzu gibt es in den Ländern unterschiedliche Regelungen. Bei den Landesrundfunkanstalten Hessischer Rundfunk, Radio Bremen und Rundfunk Berlin-Brandenburg sowie der Deutschen Welle ist die Aufsicht geteilt. Die Aufsicht über die Datenverarbeitung zu journalistischen Zwecken hat für den Hessischen Rundfunk der Beauftragte für den Datenschutz inne.

Mitglieder der RDSK sind der Rundfunkdatenschutzbeauftragte der fünf Rundfunkanstalten BR, SR, WDR, Deutschlandradio und ZDF sowie die Rundfunkdatenschutzbeauftragten des NDR, mdr, rbb, RB, des Hessischen Rundfunks und der Deutschen Welle.

Ziel der RDSK ist es, einen Beitrag zur einheitlichen Anwendung der Vorschriften der DSGVO zu leisten, insbesondere soweit es um die Anwendung im öffentlich-rechtlichen Rundfunk geht.

Den Vorsitz der RDSK hatte bis zum 31.12.2020 der Rundfunkdatenschutzbeauftragte des NDR, Herr Dr. Heiko Neuhoff, inne. Zum 01.01.2021 wurde für die Dauer von zwei Jahren der Rundfunkdatenschutzbeauftragte von BR,

SR, WDR, Deutschlandradio und ZDF, Herr Dr. Reinhart Binder, als Vorsitzender gewählt.

Im Berichtszeitraum befasste sich die RDSK insbesondere mit den folgenden Themenstellungen:

- Konsequenzen für Aufsichtsbehörden aus dem EuGH-Urteil zum Privacy-Shield
- Untersagung einer Fanpage bei Facebook
- Nutzung von Drittplattformen durch die Rundfunkanstalten
- Zusammenarbeit mit der DSK
- Anwendung von Artikel 83 DSGVO (Verhängung von Geldbußen)
- Umsetzung Artikel 35 Absatz 4 DSGVO (Blacklist DSFA)

Darüber hinaus wurden die folgenden Positionsbeschreibungen und Empfehlungen erarbeitet und veröffentlicht:

- Empfehlung der RDSK in Sachen Privacy Shield (August 2020)
- Empfehlungen der RDSK zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten (September 2020)
- Orientierungshilfe zum Einsatz webbasierter Videokonferenzsysteme (Spetember 2020)
- Datenschutzrechtliche Eckpunkte der RDSK zum Einsatz von Kollaborationssystemen (Februar 2021)
- Entschließung der RDSK zu „Clubhouse“ (Februar 2021)
- Empfehlungen zur Nutzung von Facebook-Fanpages durch die Rundfunkanstalten (März 2021)

Außerdem erfolgte im Rahmen von Videokonferenzen im Mai und Dezember 2021 ein Austausch von Mitgliedern der RDSK mit der Datenschutzkonferenz (DSK)[12]. Die Aufsichtsbehörden des Bundes, der Länder, der Kirchen und des Rundfunks besprechen in dieser Runde aktuelle Themen, wie beispielsweise aktuelle Entwicklungen im Datenschutz, Berichte über die Tätigkeitsschwerpunkte der Aufsichtsbehörden, Einsatz der Luca-App durch öffentliche Stellen sowie Kollaborationssysteme und das TTDSG.

Frankfurt am Main, im Februar 2022 gez. Ulrich Göhler

[12] DSK = Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder