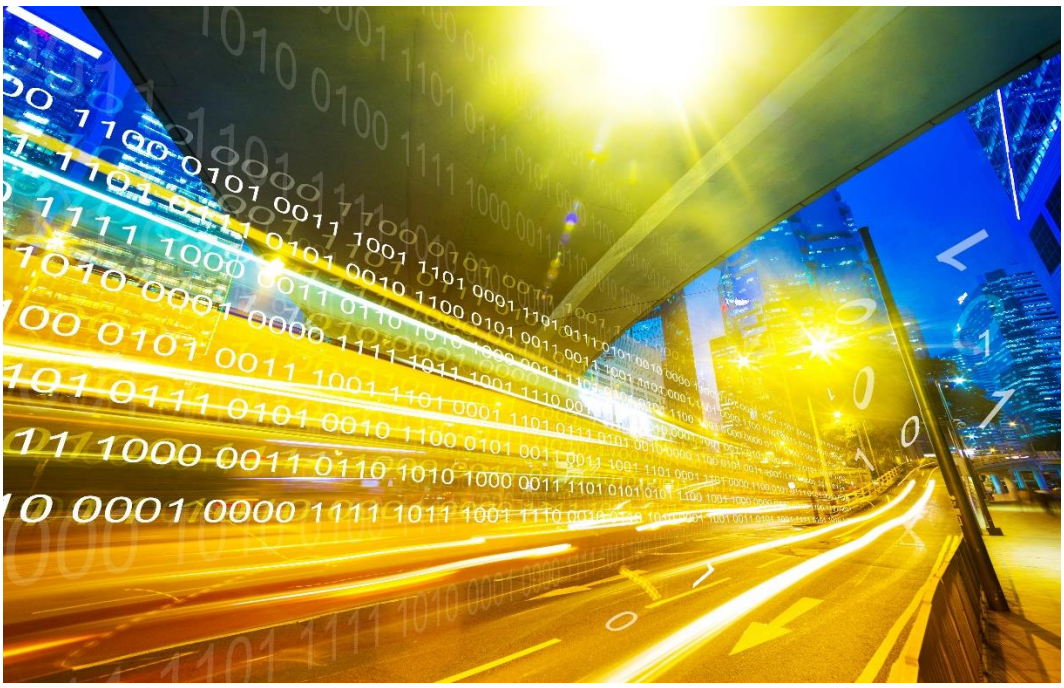
NORDDEUTSCHER RUNDFUNK

Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten des NDR

für das Berichtsjahr 2020

Dr. Heiko Neuhoff

Hamburg im Februar 2021



Vorgelegt wird hiermit der Bericht gemäß § 4 Abs. 4 NDR-Datenschutz-Staatsvertrag i. V. m. Artikel 59 der Verordnung (EU) 2016/679 (DSGVO) über die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR im Jahr 2020.

Danksagung

Für die Unterstützung des Rundfunkdatenschutzbeauftragten in allen Angelegenheiten und insbesondere bei der Erstellung dieses Berichts danke ich meiner Mitarbeiterin Frau Heike Ramand.

Inhalt

A. Einleitung

Die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR im Berichtsjahr 2020 war auch durch die Corona-Pandemie gekennzeichnet. Neben vielfältigen Fragen aus dem Regelbetrieb und zu Strukturprojekten gab es Anfragen zum Beschäftigtendatenschutz unter pandemischen Bedingungen. Die weiteren Tätigkeiten können wie folgt zusammengefasst werden:

- **Überwachung und Durchsetzung datenschutzrechtlicher Vorgaben** bei Datenverarbeitungs- und Beschaffungsvorgängen des NDR und der ARD, u. a. bei **Kollaborationssystemen** und bei der **Umsetzung höchstrichterlicher Rechtsprechung**
- **Beratung** bei Maßnahmen des NDR zum Schutz des Rechts auf informationelle Selbstbestimmung von betroffenen externen Personen und Beschäftigten
- **Bearbeitung von Anfragen und Beschwerden** des Publikums und von Rundfunkteilnehmern
- **Zusammenarbeit mit anderen Aufsichtsbehörden und Datenschutzbeauftragen**

B. Rechtsgrundlagen der Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR

Die Rechtsgrundlagen für die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR waren im Berichtsjahr unverändert. Maßgeblich sind insbesondere die seit dem 25. Mai 2018 anwendbare Datenschutzgrundverordnung (DSGVO) und der NDR-Datenschutz-Staatsvertrag. Gemäß Art. 2 Abs. 1 S. 1 NDR-Datenschutz-Staatsvertrag ist der Rundfunkdatenschutzbeauftragte Aufsichtsbehörde nach Art. 51 DSGVO und überwacht die Einhaltung der Datenschutzvorschriften bei der gesamten Tätigkeit des NDR und seiner Beteiligungsunternehmen im Sinne des § 16 c Abs. 3 Satz 1 RStV.

Aufgrund der beabsichtigten Novellierung des NDR-Staatsvertrages soll nach dem Willen des Gesetzgebers der NDR-Datenschutz-Staatsvertrag (unverändert) in den NDR-Staatsvertrages integriert werden. Darüber hinaus ist aufgrund der in Aussicht genommenen Einführung eines Informationsfreiheitsanspruches gegen den NDR aber der Tätigkeitsbereich des Rundfunkdatenschutzbeauftragten möglicherweise tangiert. Dazu wurde eine Stellungnahme abgegeben. Mehr dazu finden Sie unter Ziffer D. II. 2.

Die einschlägigen Rechtsgrundlagen sind auf der Internetseite des Rundfunkdatenschutzbeauftragten des NDR unter

https://www.ndr.de/der_ndr/unternehmen/organisation/Datenschutz-im-NDR,datenschutz6.html

zu finden.

C. Personalien

In personeller Hinsicht blieb das Datenschutzreferat unverändert: Der Verfasser dieses Berichts ist seit dem 25. Mai 2018 Rundfunkdatenschutzbeauftragter des NDR. Seit dem 1. Oktober 2018 unterstützt Frau Ramand den Rundfunkdatenschutzbeauftragten.

In den Jahren 2019 und 2020 lag der **Vorsitz des Arbeitskreises der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio (AKDSB)** und der **Vorsitz der Rundfunkdatenschutzkonferenz (RDSK) beim Rundfunkdatenschutzbeauftragten des NDR**. Regelmäßig werden die Ämter für zwei Jahre übernommen. In der Sitzung des Arbeitskreises der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio (AKDSB) am 19./20. November 2020 wurde allerdings das **Amt des Vorsitzenden des AKDSB für ein Jahr verlängert**. Zum neuen Vorsitzenden der Rundfunkdatenschutzkonferenz wurde der Rundfunkdatenschutzbeauftragte des BR, DRadio, SR, WDR und ZDF gewählt. Die damit voraussichtlich einhergehende Arbeitsentlastung ist zu begrüßen.

Die Ernennung als **stellvertretender Rundfunkbeauftragter für den Datenschutz des MDR** gemäß Art. 2 Abs. 3 der Satzung über die Rundfunkbeauftragte für den Datenschutz des MDR gilt fort. Der Fall einer Verhinderung der Rundfunkbeauftragten für den Datenschutz des MDR über einen Zeitraum von länger als 2 Monaten ist bislang nicht eingetreten.

D. Wesentliche (rechtliche) Entwicklungen im Berichtszeitraum

Das Datenschutzrecht, oder besser: das Recht auf informationelle Selbstbestimmung, ist nicht neu. Es ist auch keine „Grundrechtserfindung“, sondern eine Ausformung des allgemeinen Persönlichkeitsrechts. Jede Person hat das Recht auf freie Entfaltung der Persönlichkeit unter Garantie der Menschenwürde. Tatsächlich kommt aber dieser Dimension des

Persönlichkeitsrechts in weitgehend digitalisierten Gesellschaften eine wachsende Bedeutung zu. Denn die Digitalisierung und datenbasierte Technologien bergen neben diversen Vorteilen auch Risiken für die von Datenverarbeitungen betroffenen Personen.

Das Menschenbild des Grundgesetzes ist maßgeblich gekennzeichnet durch Eigenständigkeit, Selbstverantwortlichkeit und dem Recht zur Selbstbestimmung. Mit dem fortschreitenden Einsatz digitaler Technologien gewinnt das Recht auf informationelle Selbstbestimmung zunehmend an Gewicht. Denn dieses Recht entstammt auch aus der Garantie der Würde des Menschen, deren Unantastbarkeit durch die sogenannte Ewigkeitsgarantie des Art. 79 Abs. 3 GG abgesichert ist. Eine fremdbestimmte oder gar heimliche „Ausleuchtung“ von Personen verbietet sich daher. Damit geht einher, dass die Selbstbestimmung gewahrt und Privatheit geschützt werden müssen. Und nicht zuletzt gehört auch die Gewährleistung der Sicherheit hinzu: Die Umwandlung von Individuen in digitale Umschreibungen und Kennzeichnungen bedingt, dass diese einen ebensolchen Schutz genießen müssen wie das Individuum in seiner analogen Umwelt. Nicht zu wissen, wo man sich befindet, ist befremdlich und bedrohlich. Orientierung ist für eine Selbstbestimmung konstitutiv (weshalb sich Menschen zunehmend navigieren lassen). Umso bedenklicher ist es, wenn ein Individuum nicht (mehr) weiß, was wo von ihm ist und bekannt ist. Menschen werden im geschäftlichen und nicht privaten Umfeld und in der Kommunikation sowie der Bewältigung ihrer Angelegenheiten immer mehr in Zeichen und Daten übersetzt. Die Gefahr nicht mehr zu wissen, wo der digitale „Teil-Avatar“ des Individuums ist und was mit ihm geschieht ist groß. Datenschutz will dies verhindern und daher das Recht der Integrität einer Person wahren und schützen. Vervielfältigen, aber auch ändern und manipulieren von digitalen Daten ist leicht und die Begrenzung der Daten auf ein notwendiges Maß und einen konkreten Zweck daher unerlässlich. Dieses Ziel verfolgt das Datenschutzrecht, das fortwährend weiterentwickelt wird.

I. Gesetzgebung

Soweit der NDR bzw. der öffentlich-rechtliche Rundfunk unmittelbar betroffen ist, wird auf die wesentlichen datenschutzrechtlichen Gesetzgebungen in diesem Bericht eingegangen.

1. Medienstaatsvertrag

Nach der Zustimmung der 16 Länderparlamente ist der Medienstaatsvertrag am 7. November 2020 in Kraft getreten. Abgelöst wurde damit der Rundfunkstaatsvertrag, um eine umfassende Reform der Medienordnung vorzunehmen. Im Medienstaatsvertrag finden sich fast unverändert Vorschriften zum Mediendatenschutz, der nunmehr insbesondere im Medienstaatsvertrag und der DSGVO sowie dem NDR-Datenschutz-Staatsvertrag zu finden ist. Zuständigkeiten und Kompetenzen bleiben danach unangetastet. So heißt es in § 12 Abs. 4 MedienStV:

> *„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."*

2. NDR-Staatsvertrag

Ende Oktober 2020 haben die vier Staatsvertragsländer des NDR den Entwurf eines neuen NDR-Staatsvertrages präsentiert. In der Synopse zum neuen Staatsvertrag (https://www.regierung-mv.de/static/Regierungsportal/Portalredaktion/NDR-Synopse.pdf) werden in der linken Spalte in den §§ 41, 42 NDR-StV datenschutzrechtliche Vorschriften abgebildet, die bereits mit dem am 25. Mai 2018 in Kraft getretenen NDR-Datenschutz-StV gestrichen wurden. Ein Vergleich der Regelungen des NDR-Datenschutz-StV mit den einschlägigen Vorschriften des Entwurfs des NDR-StV (§§ 43 bis einschließlich 46) ergab, dass die Vorschriften des derzeit geltenden NDR-Datenschutz-StV ohne inhaltliche oder sprachliche Änderungen in den §§ 43 bis einschließlich 46 des Entwurfs des NDR-StV eingefügt wurden.

Im Rahmen des Anhörungsverfahrens der Länder Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein zur beabsichtigten Neufassung des Staatsvertrags über den Norddeutschen Rundfunk (NDR) in seiner derzeit gültigen Fassung vom 1./2. Mai 2005 hatte der Verfasser dieses Berichts dazu gemäß Art. 58 Abs. 3 lit. b) DSGVO Stellung genommen und mitgeteilt, dass sich die seit rund 2,5

Jahren geltenden Vorschriften rechtlich und in der Praxis bewährt haben und etwaiger Anpassungsbedarf nicht ersichtlich ist.

Im Entwurf des NDR-StV ist beabsichtigt erstmals zu regeln, dass es einen Zugang zu Informationen für natürliche und (inländische) juristische Personen unter bestimmten Voraussetzungen geben soll. Auch dazu wurde wie folgt Stellung genommen:

„Über etwaig vom NDR abgelehnte Anträge auf Informationen sollen nach § 47 Absatz 11 die jeweiligen Datenschutzbeauftragten der Länder entscheiden. Dies ist zum einen systemwidrig, zum anderen unzutreffend eingeordnet. Dies deshalb, weil gemäß § 4 NDR-Datenschutz-Staatsvertrag (und § 46 des identisch lautenden Entwurfs des NDR Staatsvertrags) die/der Rundfunkdatenschutzbeauftragte die Vorschriften über den Datenschutz bei der gesamten Tätigkeit des NDR überwacht. Dies bezieht die Überwachung des Datenschutzes für Mitarbeitende und Dritte ein, die bspw. durch (redaktionelle) Datenverarbeitungen des NDR betroffen sind (vgl. § 1 NDR-Datenschutz-Staatsvertrag und § 43 des identisch lautenden Entwurfs des NDR-Staatsvertrags). Eine Zuständigkeit der Landesdatenschutzbeauftragten über die Tätigkeit des NDR und seiner Hilfs- und Beteiligungsunternehmen ist insgesamt nicht eröffnet.

Die grundrechtlich bedingte Autonomie des öffentlich-rechtlichen Rundfunks gebietet nicht nur in inhaltlicher Hinsicht Staatsferne im Sinne einer Nichteinmischung staatlicher Stellen in die Programmgestaltung des öffentlich-rechtlichen Rundfunks. Auch die Organisation der öffentlich-rechtlichen Rundfunkanstalten muss gemäß der für die Rundfunkfreiheit wesentlichen Konzeption des Grundrechtsschutzes durch Verfahren staatsfern erfolgen. Das Selbstverwaltungsrecht der öffentlich-rechtlichen Rundfunkanstalten ist daher die notwendige Konsequenz aus dem verfassungsrechtlichen Gebot der Staatsferne des öffentlich-rechtlichen Rundfunks.

Da der NDR Träger des Grundrechts der Rundfunkfreiheit ist, besitzt er notwendig auch das Recht zur Selbstverwaltung. Dies hat auch für die Stellung der/des Rundfunkdatenschutzbeauftragten beim öffentlich-rechtlichen Rundfunk Folgen, die sich in den Regelungen des NDR-Datenschutz-StV bzw. den gleichlautenden Vorschriften des Entwurfs des NDR-StV (§§ 43 bis einschließlich 46) niederschlagen: Ebenso wie die Landesdatenschutzbeauftragten ist auch die/der Rundfunkdatenschutzbeauftrag-

te in der Ausübung ihres/seines Amtes unabhängig und nur dem Gesetz unterworfen. Sie/Er besitzt eine richterähnliche Stellung. Gegenüber staatlichen Behörden kann sich die/der Rundfunkdatenschutzbeauftragte auf die Staatsferne der öffentlich-rechtlichen Rundfunkanstalt berufen und damit die Kontrolle ihrer/seiner Tätigkeit durch weitere staatliche Stellen verhindern. In ihrer/seiner Funktion als Rundfunkdatenschutzbeauftragter können daher auch von keiner Seite, weder innerhalb noch außerhalb der Rundfunkanstalt, Weisungen erteilt werden.

Die im Entwurf enthaltenen Kompetenzen der Landesdatenschutzbeauftragten sind daher der Aufsicht des NDR wesensfremd und überdies auch nicht in den Zuständigkeiten der Landesdatenschutzbeauftragten enthalten (vgl. etwa §§ 18 Abs. 1; 19 Abs. 1 Niedersächsisches Datenschutzgesetzes (NDSG)), da die Aufsichtsbefugnisse der/des Rundfunkdatenschutzbeauftragten mit denen der Landesdatenschutzbeauftragten identisch sind und die Abgrenzung und der Aufgabenbereich bereits abschließend in § 4 NDR-Datenschutz-Staatsvertrag (und § 46 des identisch lautenden Entwurfs des NDR Staatsvertrags) geregelt sind. Zudem wäre insbesondere mit der Regelung des § 47 Abs. 9 Ziffer 1 eine doppelte Kompetenz eröffnet. Überdies sind teilweise Zuständigkeiten von Landes- oder Bundesdatenschutzbeauftragten bezüglich des öffentlich-rechtlichen Rundfunks systemwidrig und verfassungsrechtlich bedenklich, weil journalistisch-redaktionelle Belange in der Praxis nicht von Verwaltungsaufgaben zu trennen sind."

Diese Auffassung wird mehrheitlich vertreten. So hat etwa der Bundesgesetzgeber im Rahmen der Umsetzung der DSGVO (DSAnpUG-EU vom 30.6.2017; BGBl 2017,2097 ff.) in der Gesetzesbegründung ausdrücklich festgehalten, dass es geboten sei, den

> *„Begriff ‚journalistisch' weit auszulegen, so dass auch diejenigen Voraussetzungen und Hilfstätigkeiten eingeschlossen sind, ohne welche die Medien ihre Funktion nicht in angemessener Weise erfüllen können (vgl. BVerfG, Urteil vom 12.03.2003, 1 BvR 330/96, Rdnr. 103). Hiervor können auch Verwaltungstätigkeiten und sonstige Hilfstätigkeiten erfasst sein, soweit diese Rückwirkungen auf die journalistische Tätigkeit haben können"... „Ziel ist es, der Bedeutung des Rechts auf freie Meinungsäußerung und Informationsfreiheit in einer demo-*

kratischen Gesellschaft Rechnung zu tragen“ (BTags-Drs. 19/4674 vom 1.10.2020, S. 258 und 259 zur Deutschen Welle).

3. e-Privacy-Verordnung und Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)

Die e-Privacy-Verordnung (VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)) gibt es noch immer nicht, obwohl sie bereits im Mai 2018 in Kraft treten sollte. Regelungsgegenstände einer solchen Verordnung wären insbesondere der Einsatz von Cookies und das Nutzertracking auf Internetseiten zwecks Stärkung der Privatsphäre der Nutzer*innen. Derzeit soll ein Entwurf der Portugiesischen Ratspräsidentschaft existieren. Details sind noch nicht bekannt.

Ein Referentenentwurf vom 14. Dezember 2020 des Bundesministeriums für Wirtschaft und Energie und des Bundesministeriums für Verkehr und digitale Infrastruktur enthält den „Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz)“. Zu datenschutzrechtlichen Regelungen heißt es dort:

> *„Der bislang in § 88 festgeschriebene Schutz des Fernmeldegeheimnisses wird künftig in einem gesonderten Gesetz [Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikations-Telemedien-Datenschutz-Gesetz -TTDSG)] geregelt. Dementsprechend wird das diesbezügliche Ziel, die Wahrung des Fernmeldegeheimnisses, an dieser Stelle gestrichen.“*
>
> *„Der bisherige Teil 7 „Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit“ wurde grundlegend überarbeitet. Aufgrund verschiedener unionsrechtlicher Vorgaben werden die Abschnitte „Fernmeldege-*

heimnis“ und „Datenschutz“ aus dem TKG herausgelöst und in das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) überführt. Datenschutzrechtliche Vorgaben für die im TKG geregelten Datenverarbeitungsplichten ergeben sich insofern künftig neben dem BDSG und der DSGVO auch aus dem TTDSG.“

Mit dem in Aussicht genommenen TTDSG sollen Vorschriften aus der DSGVO, dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) harmonisiert und die Datenschutzbestimmungen zusammengeführt werden, um mehr Rechtsklarheit zu gewinnen. Die Regelungsbereiche einer e-Privacy-Verordnung und eines TTDSG würden sich in weiten Teilen decken und beide Regelwerke könnten sich auf die Telemedienangebote des öffentlich-rechtlichen Rundfunks auswirken.

II. Rechtsprechung

Die Anzahl gerichtlicher Entscheidungen zum Datenschutz nimmt zu. Von Bedeutung für den NDR und den öffentlich-rechtlichen Rundfunk waren im Jahr 2020 die folgenden Urteile.

1. EuGH-Entscheidung zum EU-US-Privacy Shield

Am 16. Juli 2020 hat der EuGH entschieden, dass das sog. „EU-US-Privacy Shield“ ungültig ist. Aus dieser Entscheidung ergaben sich auch Konsequenzen für den NDR, sofern er nach der Aufhebung des Privacy Shields (weiterhin) die Übermittlung personenbezogener Daten in die USA vornimmt oder veranlasst.

Hintergrund der Entscheidung war Folgendes: Die DSGVO stellt verschiedene Instrumente zur Übermittlung personenbezogener Daten in Drittländer bereit. Ein solches Instrument war das EU-US-Privacy Shield als sog. Angemessenheitsbeschluss im Sinne von Art. 45 DSGVO. Mit solchen Angemessenheitsbeschlüssen beurteilt die Europäische Kommission das datenschutzrechtliche Schutzniveau in Staaten außerhalb der EU und spricht aus, ob das Datenschutzniveau jenem der EU gleichwertig ist. Die EU hatte die US-Datenschutzregeln im Privacy-Shield als angemessen angesehen. Der EuGH hat hingegen festgestellt, dass das Datenschutzniveau in den USA wesentlich geringer („schlechter“) ist, weil das Abkommen „den Erfordernissen der nationa-

len Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang“ einräume und „die auf die amerikanischen Rechtsvorschriften gestützten Überwachungsprogramme nicht auf das zwingend erforderliche Maß beschränkt“ seien. Der EuGH hat daher das Privacy-Shield mit sofortiger Wirkung aufgehoben.

Da das Datenschutzniveau in den USA nach den Feststellungen des EUGH insgesamt zu gering ist, kann seit dem Urteil nicht mehr unter Bezugnahme auf das Privacy-Shield eine Übertragung von personenbezogenen Daten in die USA vorgenommen werden. Ein weiteres Instrument zur Datenübertragung in die USA sind sog. Standardvertragsklauseln. Dies sind standardisierte Verträge, von der Europäischen Kommission erlassene Vertragsmuster, in denen die datenschutzrechtlichen Pflichten der beteiligten Unternehmen festgelegt werden. Grundsätzlich stellen Standardvertragsklauseln ein geeignetes Mittel zur Übermittlung von personenbezogenen Daten in Länder außerhalb der EU dar. Jedoch hat der EuGH in seiner Entscheidung diesbezüglich festgestellt, dass diese nicht ohne Weiteres für Datenübertragungen in die USA geeignet sind, weil aufgrund der US-Gesetzgebung das Datenschutzniveau auch durch vertragliche Vereinbarungen von Unternehmen nicht erhöht wird.

Der EuGH meint allerdings, dass durch die sofortige Aufhebung des Privacy Shields nicht zwingend ein rechtliches Vakuum entstehen müsse, weil für Ausnahmefälle (gelegentliche und nicht wiederholte Übermittlungen) Handlungsspielraum bliebe.

Bereits im Tätigkeitsbericht für das Jahr 2019 wurde darauf hingewiesen, dass es wünschenswert sei, dass auch in den USA und Asien ähnliche Regulierungsmodelle wie in der EU etabliert werden, weil Datenverarbeitungen vermehrt außerhalb des europäischen Rechtsraums vorgenommen werden. Wie sich der internationale datenschutzrechtliche Regulierungsrahmen aufgrund dieses entwickelt, bleibt abzuwarten. Hoffnungsvoll stimmt, dass in Kalifornien im Wege eines Volksentscheids vom 30. November 2020 die erste Datenschutzbehörde eingerichtet wurde.

Zu den Konsequenzen aus der Entscheidung und der Tätigkeiten der Aufsichtsbehörden siehe Ziffer E. I. 1. b), E. II. 2. e) und E. II. 5. b) dieses Berichts.

2. BGH-Entscheidung zur Einwilligung in die Verwendung von Cookies

Mit Urteil vom 1.10.2019 (Az. C-673/17) hatte der EuGH eine Entscheidung zur Notwendigkeit von Einwilligungen der Nutzer*innen in die Verwendung von Cookies gefällt. Im Jahr 2020 hat nun der BGH dazu ein Urteil gesprochen.

Der Europäische Gerichtshof (EuGH) hatte die Anforderungen an eine wirksame Einwilligung zur Speicherung von oder den Zugriff auf Informationen spezifiziert, die bereits im Endgerät des Nutzers einer Website gespeichert sind. Der BGH entschied nun mit Urteil vom 28. Mai 2020 (Az. I ZR 7/16), dass diese Grundsätze auch für Cookies gelten, die Dienstanbieter einsetzen, um mithilfe von Pseudonymen Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien zu erstellen. Gemäß § 15 Abs. 3 Telemediengesetz (TMG) können Cookies zu diesen Zwecken zwar dem Wortlaut nach vorbehaltlich eines ausdrücklichen nutzerseitigen Widerspruchs zulässig sein. Dies interpretiert der BGH jedoch im Sinne der Vorgaben von Art. 5 Abs. 3 e-Privacy-Richtlinie als Einwilligungserfordernis.

Die Rundfunkdatenschutzkonferenz hat sich mit diesem Thema befasst. Auf die Konsequenzen aus dieser Entscheidungen und weitere Einzelheiten wird daher unter Ziffer E. I. 1. b) und E. II. 2. d) eingegangen.

3. Arbeitsrecht

Ein Beschäftigtendatenschutzgesetz gibt es noch immer nicht. Die Öffnungsklausel des Art. 88 DSGVO eröffnet die Möglichkeit des Erlasses eines solchen Gesetzes, um das jeweilige nationale Recht zum Beschäftigtendatenschutz zu spezifizieren. Derweil mehren sich die Entscheidungen mit Bezug zum Datenschutz. So entschied das Landesarbeitsgericht Köln (Urteil vom 07.02.2020, Az. 4 Sa 329/19), dass die private Nutzung von Internet und E-Mail am Dienst-PC trotz eines entsprechenden Verbots während der Arbeitszeit dann eine fristlose Kündigung rechtfertigt, wenn der Arbeitnehmer sowohl an mehreren Tagen durchgehend und als auch über Monate hinweg regelmäßig URL-Aufrufe und E-Mails zu privaten Zwecken getätigt hat. Dies gelte umso mehr, wenn zwischen den einzelnen URL-Aufrufen ein Zeitraum von weniger als ein bis zwei Minuten liegt, denn dazwischen kann keine Arbeitsleistung erbracht worden sein. In diesem Fall der sehr extensiven privaten Internetnutzung durfte der Arbeitge-

ber auch überprüfen, „ob eine gegen arbeitsvertragliche Vereinbarungen verstoßende regelwidrige Internutzung erfolgt, was anhand der URLs der aufgerufenen Webseiten und der empfangenen und erhaltenen E-Mails festgestellt werden kann. Hierdurch kann auch auf einen ggf. fehlenden dienstlichen Bezug und damit einer privaten Nutzung des Internets geschlossen werden. Anhand des protokollierten Zeitpunktes des Aufrufs kann überprüft werden, ob der Aufruf während oder außerhalb der Arbeitszeit erfolgte."

Auch beschäftigen sich die Arbeitsgerichte mit sogenannten „Backgroundchecks" von Bewerber*innen. Wie weit diese gehen dürfen, ist höchstrichterlich noch nicht geklärt. Das LAG Baden-Württemberg (Urteil vom 21.02.2019, Az. 3 Sa 65/17) entschied, dass Unstimmigkeiten in den Angaben von Bewerber*innen und Arbeitnehmer*innen über den beruflichen Werdegang entsprechende Aufklärungsmaßnahmen unter Verwendung frei zugänglicher Quellen rechtfertige. Bei bestehenden Arbeitsverhältnissen muss einer entsprechenden Datenerhebung ein konkreter Verdacht einer Straftat bzw. einer erheblichen Pflichtverletzung zugrunde liegen.

Umstritten ist noch immer der Umfang des Auskunftsanspruchs nach Art. 15 DSGVO im Beschäftigtenverhältnis. Manche Gerichte neigen zu einer sehr weiten Auslegung dieses Rechts (so etwa das LAG Baden-Württemberg, Urteil vom 20.12.2018, Az. 17 Sa 11/18). Eine Entscheidung des Bundesarbeitsgerichts steht noch aus, da sich in dieser Sache die Parteien verglichen hatten und die Revision sich damit erledigte. Strittig bleibt damit der Umfang des Auskunftsrechts und das Verhältnis dieses zum Recht auf Einsicht in die Personalakte.

4. Gerichtliche Kontrolle einer aufsichtsbehördlichen Entscheidung

Entscheidungen von erstinstanzlichen Gerichten hatte es bereits gegeben, nun hat das Oberverwaltungsgericht Rheinland-Pfalz mit Urteil vom 26.10.2020 (Az. 10 A 10613/20) Folgendes bestätigt:

Erhebt eine betroffene Person eine Beschwerde wegen einer behaupteten Datenschutzverletzung, muss sich die Datenschutz-Aufsichtsbehörde (im entschiedenen Fall der Landesdatenschutzbeauftragte Rheinland-Pfalz) mit der Beschwerde befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und

den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung und ergänzend über die Möglichkeit eines gerichtlichen Rechtsbehelfs unterrichten.

Eine inhaltlich-materielle gerichtliche Überprüfung der Entscheidung der Aufsichtsbehörde sieht die DSGVO nicht vor, da es sich bei dem Beschwerderecht gemäß Art. 77 DSGVO um ein petitionsähnliches Recht handele, das nur einer eingeschränkter richterlichen Kontrolle unterliegt.

Dem Beschwerdeführer bleibt neben dem Beschwerderecht gegenüber der Aufsichtsbehörde die Möglichkeit, nach Maßgabe des Art. 79 DSGVO sich unmittelbar an den Verantwortlichen zu wenden. Im Gegensatz zum Beschwerdeverfahren sind derartige Verfahren kontradiktorisch, weil zwischen dem Verantwortlichen und dem Betroffenen eine rechtsverbindliche Klärung vorgenommen wird, ob der Betroffene durch einen datenschutzrechtlichen Verstoß des Verantwortlichen in seinen Rechten verletzt wurde.

E. Tätigkeiten des Rundfunkdatenschutzbeauftragten im Berichtszeitraum

Es folgen die Tätigkeiten bezüglich der Zusammenarbeit mit anderen Aufsichtsbehörden, insbesondere der Rundfunkdatenschutzkonferenz (kurz: RDSK – den Datenschutzbeauftragten im öffentlich-rechtlichen Rundfunk) und der Datenschutzkonferenz der Länder (DSK).

I. Organisationsstrukturen/Zusammenarbeit mit anderen Aufsichtsbehörden

Im Jahr 2019 wurde der Zusammenschluss der als Aufsichtsbehörden tätigen Personen im öffentlich-rechtlichen Rundfunk, die Rundfunkdatenschutzkonferenz (RDSK) gegründet. Daneben gibt es den Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio (AKDSB) als Expertenforum zum Austausch über gemeinsame Belange und zur Beratung und Begleitung des operativen Geschäfts der Rundfunkanstalten und Gemeinschaftseinrichtungen. Die Datenschutzkonferenz (DSK) ist das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Mit der DSK finden Regelsitzungen statt. Zudem besteht die Möglichkeit an Arbeitskreisen der DSK teilzunehmen.

1. Die Rundfunkdatenschutzkonferenz (RDSK)

Die RDSK besteht weiterhin aus 8 Personen. Sie üben die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk über die Rundfunkanstalten und deren Gemeinschaftseinrichtungen und Beteiligungsunternehmen aus. Mitglieder der RDSK sind

- der Rundfunkdatenschutzbeauftragte des Bayerischen Rundfunks, des Saarländischen Rundfunks, des Westdeutschen Rundfunks, des Deutschlandradios und des Zweiten Deutschen Fernsehens,
- der Datenschutzbeauftragte des Hessischen Rundfunks,
- der Rundfunkbeauftragte für den Datenschutz beim Mitteldeutschen Rundfunk,
- der Rundfunkdatenschutzbeauftragte des Norddeutschen Rundfunks,
- die Datenschutzbeauftragte von Radio Bremen,
- die Datenschutzbeauftragte des Rundfunk Berlin-Brandenburg,
- der Rundfunkbeauftragte für den Datenschutz beim Südwestrundfunk und
- der Datenschutzbeauftragte der Deutschen Welle.

a) Organisation der RDSK

Die Aufgaben und Funktion der RDSK sind in der **Geschäftsordnung** festgelegt. Neben der Geschäftsordnung haben im Jahr 2020 die Mitglieder der RDSK zwei Verwaltungsvereinbarungen in Kraft gesetzt:

Die „**Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten**“ regelt die Wahrnehmung der Datenschutzaufsicht über die Unternehmen, an denen die von ihnen zu beaufsichtigenden Rundfunkanstalten insgesamt oder teilweise unmittelbar oder mittelbar gemeinschaftlich beteiligt sind (Gemeinschaftsunternehmen). Es wird geregelt, dass die Aufsicht über jedes Gemeinschaftsunternehmen eine Aufsichtsbehörde federführend wahrnimmt. Ihre Handlungen und Erklärungen wirken im Verhältnis zum Gemeinschaftsunternehmen für und gegen die anderen Aufsichtsbehörden.

Die Aufgaben und Befugnisse jeder beteiligten Aufsichtsbehörde nach den Art. 57 f. DSGVO bzw. den jeweils maßgeblichen gesetzlichen Vorschriften bleiben von einer Federführung unberührt.

Im Einzelnen werden die Zuständigkeiten der federführenden Aufsichtsbehörde und die Abstimmungserfordernisse sowie der Informationsaustausch zwischen dem Federführer und den anderen Aufsichtsbehörden festgelegt.

In gleicher Weise wird dies auch geregelt für die rechtlich nicht selbständigen Gemeinschaftseinrichtungen in der „**Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten**“.

Die Verwaltungsvereinbarungen gelten zunächst bis zum 31. Dezember 2022. Sie verlängern sich um jeweils ein weiteres Jahr, sofern nicht eine der Vertragsparteien spätestens zum 30. September eines Kalenderjahres kündigt.

Öffentlichkeitsarbeit, Vernetzung und inhaltliche Positionierungen durch entsprechende Empfehlungen, Stellungnahmen und Orientierungshilfen sind Kernaufgaben der RDSK. Im Jahr 2021 dürfte dazu die Internetseite der RDSK freigeschaltet werden können. Die entsprechenden Vorbereitungen wurden im Berichtsjahr getroffen. Das Logo der RDSK sieht wie folgt aus:

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

b) Tätigkeitsschwerpunkte der RDSK

Die RDSK hat sich im Jahr 2020 dreimal zusammengeschaltet. Präsenzsitzungen konnten aus pandemischen Gründen nicht abgehalten werden. Insgesamt liegen nun 5 Papiere der RDSK vor:

- Positionspapier der RDSK zum IP-Autostart bei der Nutzung von HbbTV
- Einsatz cloudbasierter Office-Systeme: Datenschutzrechtliche Eckpunkte
- Empfehlung der Konferenz der Datenschutzaufsichten im öffentlich-rechtlichen Rundfunk zum Verfahren CDDC (Custom Domain Data Collection)
- Empfehlungen der RDSK zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten
- Datenschutzbeauftragte in Gemeinschaftseinrichtungen und gemeinschaftlichen Beteiligungsunternehmen der Rundfunkanstalten

Weitere Papiere, etwa eine Empfehlung der RDSK zu Videokonferenzsystemen und Stellungnahmen zu Gesetzgebungsvorhaben, sind in Arbeit. Gegenstand fortwährender Betrachtung sind überdies die Entscheidung zur Untersagung einer Fanpage bei Facebook und etwaige Weiterungen mit Blick auf andere Auftritte der Rundfunkanstalten in sozialen Medien.

Schwerpunkte waren die Folgerungen aus den Entscheidungen des EuGH zum Wegfall des Privacy Shields und des BGH zum Einsatz von Cookies: Die bereits auf der Basis der Entscheidung existierende „**Empfehlung der RDSK zum Einsatz von Cookies**“ war aufgrund des Urteils des BGH vom 28.05.2020 zu aktualisieren. Die Schlussfolgerungen lassen sich wie folgt zusammenfassen:

- **Rechtsgrundlage prüfen**
  Die Rundfunkanstalten sollten jedes von ihnen eingesetzte Cookie darauf überprüfen, ob sie es auf einen Erlaubnistatbestand stützen können. Dies kann einer der in Art. 6 Abs. 1 S. 1 lit. b) – f) DSGVO genannten Tatbestände oder eine Einwilligung der betroffenen Person sein.

- **Wirksamkeit der Einwilligungserklärung sichern**
  Die Rundfunkanstalten sollten die von ihnen eingesetzten Tools, mithilfe derer sie die im Regelfall erforderliche Einwilligung der betroffenen Person einholen, daraufhin überprüfen, ob sie die Anforderungen erfüllen, die sich aus Art. 4 Nr. 11, Art. 7 und ggf. Art. 8 DSGVO sowie der Rechtsprechung des EuGH ergeben.
- **Datenschutzerklärung/Cookie-Hinweis anpassen**
  Die Datenschutzerklärung muss Hinweise zur Funktion des jeweiligen Cookies mit mindestens allen Angaben enthalten, die Art. 13 DSGVO fordert.
- **Spezifische Aufgabe des öffentlich-rechtlichen Rundfunks erklären**
  Zu Recht erwarten die Nutzer*innen vom öffentlich-rechtlichen Rundfunk einen besonders hohen Datenschutzstandard. Da im allgemeinen gerade Cookies, die das Nutzungsverhalten erfassen und auswerten, nur mit ausdrücklicher Einwilligung der betroffenen Person eingesetzt werden dürfen, entsteht erhöhter Aufklärungs- und Beratungsbedarf, wenn die Rundfunkanstalten weiterhin für einzelne Cookies keine Einwilligung einholen. Sie sollten daher ihre Datenschutzerklärungen bzw. Cookie-Hinweise besonders sorgfältig und verständlich formulieren. Allgemeinplätze wie etwa das Bestreben, mithilfe eines Cookies „den Nutzer*innen ein bestmögliches Angebot zur Verfügung zu stellen“, werden dem nicht gerecht. Insbesondere sollten die Rundfunkanstalten daher die spezifische Aufgabe und Funktion des öffentlich-rechtlichen Rundfunks erläutern und die sich daraus ergebende Rechtsgrundlage für den Einsatz des betreffenden Cookies nennen.

Weiterhin waren die **Konsequenzen für Aufsichtsbehörden aus dem EuGH-Urteil zum Wegfall des Privacy-Shield** zu erörtern und Empfehlungen für das weitere Vorgehen der Verantwortlichen auszusprechen. Diese lauten wie folgt:

- 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.

- 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.
- 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.
- 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.

- Die Feststellungen des Gerichtes beziehen sich allein auf das 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.
- 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.

c) Zusammenarbeit mit der Datenschutzkonferenz

Im Oktober 2020 gab es einen Austausch mit der **Datenschutzkonferenz** (DSK), dem Gremium der Datenschutzaufsichtsbehörden des Bundes und der Länder. Die Aufsichtsbehörden der Länder, des Bundes, der Kirchen und des Rundfunks haben aktuelle Themen besprochen: Der Vorsitzende der DSK hat über Aktivitäten und Entscheidungen der DSK im Jahr 2020 berichtet, ebenso über die Medizininformatik-Initiative des Bundes. Auch war in diesem Kreise das Urteil des EuGH vom 16. Juli 2020 (Privacy-Shield) Thema sowie ein Bericht aller Aufsichtsbehörden zur Verarbeitung personenbezogener Daten bei der Bewältigung der Corona-Pandemie.

Zudem haben Mitglieder der RDSK an den Arbeitskreisen AK Technik, AK Grundsatzfragen und AK Medien der Datenschutzkonferenz teilgenommen. Es gilt weiterhin, dass der Austausch zu begrüßen, aber auch zu intensivieren ist. Der Vielzahl von Themen mit datenschutzrechtlicher Relevanz kann nur durch das in Art. 51 DSGVO niedergelegte Gebot der Zusammenarbeit und Kohärenz begegnet werden.

2. Der Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des DRadio

Die regelmäßigen Präsenzsitzungen AKDSB wurden im Jahr 2020 durch Videokonferenzen ersetzt. Dreimal haben sich die Mitglieder des AKDSB ausgetauscht. Die Schwerpunkte waren folgende Themen:

- Konsequenzen aus dem EuGH-Urteil zum Wegfall des Privacy Shields/Übermittlung von personenbezogenen Daten in die USA
- Brexit: Handlungsbedarfe für die Rundfunkanstalten
- Entwicklungen auf europäischer Ebene: Überblick über die Aktivitäten der EU
- die Novellierung des IT-Sicherheitsgesetzes
- Datenschutz beim Beitragsservice:
  - Beschäftigtendatenschutz und Corona
  - Sachbearbeitung von Teleheimarbeitsplätzen beim Beitragsservice
  - die Überarbeitung der Beitragseinzugsordnung des Beitragsservice
  - Löschkonzepte des Beitragsservice
  - die Umsetzung des 23. Rundfunkänderungsstaatsvertrages beim Beitragsservice
  - das Kundenkontaktmanagement beim Beitragsservice
  - Sachstand zum Projekt X-Amtshilfe (Bundesweiter Inhaltsdatenstandard für den Daten- und Informationsaustausch zu Amtshilfeersuchen)
- Vereinbarungen zur gemeinsamen Verantwortlichkeit beim IVZ und beim ARD-Sternpunkt
- Überarbeitung des Musters für Auftragsverarbeitungen
- Klassifizierungen von Datenkategorien und deren Schutzbedarfe
- EDV-Harmonisierungsprojekte der ARD
- Datenschutz und Datenverarbeitungen in der Cloud, Cloud Telefonie

- die Einführung eines SIEM/SOC (Security Information and Event Management, Security Operations Center)
- Videokonferenzsysteme
- das Medienprivileg
- Nutzungsmessungen und Datenschutz
- die Etablierung eines Verfahrens für Informationssicherheit und Risikoanalyse auf ARD-Ebene
- Beschäftigtendatenschutz
- Datenschutzschulungen der Medienakademie
- Kinderangebote über Sprachassistenten

Der Verfasser des Berichts war der **Vorsitzende des AKDSB** und hat Termine koordiniert, Tagesordnungen und Sitzungen vorbereitet und die Zusammenkünfte geleitet.

Erfreulicherweise ist es gelungen, die notwendigen Vereinbarungen nach Art. 26 DSGVO (sog. **Joint Controller Vereinbarungen**) für die Gemeinschaftseinrichtungen

- Beitragsservice,
- Informations-Verarbeitungs-Zentrum (IVZ),
- ARD-Sternpunkt

in Kraft zu setzen. Der rechtliche Hintergrund der Vereinbarungen findet sich in Art. 26 DSGVO. Nach dieser Vorschrift müssen die gemeinsam für die Verarbeitung personenbezogener Daten Verantwortlichen in einer Vereinbarung in transparenter Form festlegen, wer von Ihnen welche der sich aus der DSGVO ergebenden Verpflichtungen erfüllt, etwa

- die Erfüllung von Betroffenenrechten,
- das Führen des Verzeichnisses der Verarbeitungstätigkeiten,
- die Sicherstellung der Datensicherheit durch geeignete technisch-organisatorische Maßnahmen,
- die Meldekette für den Fall meldepflichtiger Verstöße.

Hinsichtlich des IVZ und des ARD-Sternpunktes wurde jeweils der Forderung des AKDSB entsprochen, betriebliche Datenschutzbeauftragte einzusetzen (für den Beitragsservice gibt es eine gesetzliche Verpflichtung, vgl. § 11 Abs. 2 Rundfunkbeitragsstaatsvertrag).

Viele Kapazitäten binden darüber hinaus EDV-Harmonisierungsprojekte und hier namentlich ein ARD-Strukturprojekt, mit dem für alle ARD-Anstalten und das Deutschlandradio die **Harmonisierung und Konsolidierung der Geschäftsprozesse und der dezentralen SAP-Systeme der einzelnen Rundfunkanstalten in eine zentrale SAP Systemlandschaft** beabsichtigt ist. Die dabei auftretenden datenschutzrechtlichen Fragestellungen sind vielfältig und komplex und werden weiterhin Beratungsbedarf auslösen. Die datenschutzrechtliche Befassung mit diesem Projekt war nicht nur im AKDSB ein Schwerpunkt. Das Projekt ist äußert umfangreich und vielschichtig, zumal es sich in diverse Unterprojekte gliedert, die jeweils datenschutzrechtliche Relevanz aufweisen. Die Landesrundfunkanstalten und das Deutschlandradio haben sich nämlich zum Ziel gesetzt, ihre betriebswirtschaftlichen Prozesse einschließlich der technischen Systeme, mit denen sie elektronisch verarbeitet werden, zu harmonisieren. Dazu sollen die Systeme und Anwendungen vereinheitlicht werden. Die einzelnen Projekte und Module gliedern sich in übergeordnete Komplexe und Anwendungen auf, beispielsweise

- Migrationskonzepte,
- Löschkonzepte,
- Schnittstellenmanagements,
- Stammdatenkonsolidierungen,
- Anwendungsmanagement- und Verwaltungslösungen zur Implementierung, Unterstützung, Bedienung und Überwachung weiterer Anwendungen,
- Cloud-Anwendungen

und in einzelne Geschäftsbereiche, wie zum Beispiel

- Finanzen,
- Controlling,
- Beschaffung, Warenwirtschaft, Vertragswesen,
- Cloud-Anwendungen,
- Dienstreisen,

- E-Procurement.

II. Tätigkeitsschwerpunkte bezüglich Datenverarbeitungen im NDR

Im Erwägungsgrund 129 der DSGVO heißt es:

„Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedsstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter, insbesondere im Fall von Beschwerden natürlicher Personen, Untersuchungsbefugnisse, Abhilfebefugnisse und Sanktionsbefugnisse und Genehmigungsbefugnisse und beratende Befugnisse, […]."

Der Schwerpunkt der Tätigkeit lag, wie in den Jahren zuvor auch, auf den **Beratungen von bestehenden und beabsichtigten Datenverarbeitungstätigkeiten**. Überwiegend wird der Rundfunkdatenschutzbeauftragte um Beratung gebeten und kann so die jeweiligen Anforderungen des Rechts auf informationelle Selbstbestimmung formulieren und von etwaigen Sanktionen absehen.

Wie im Jahr zuvor auch, werden die Tätigkeiten des Berichtsjahrs wie folgt vorgestellt:

- Programm und Programmverbreitung,
- Rundfunkteilnehmerdatenschutz,
- Beschäftigtendatenschutz,
- weitere Organisations- und Strukturprojekte.

Dem **Beschäftigtendatenschutz** kam pandemisch bedingt im Jahr 2020 eine besondere Rolle zu. Der **Beratungsbedarf bei Organisations- und Strukturprojekten** ist stetig hoch, wobei das Thema „Collaboration" ein Schwerpunkt war (und bleiben wird).

1. Zur Umsetzung der DSGVO

Am 24. Juni 2020 veröffentliche die EU-Kommission einen Bericht zur Bewertung und Überprüfung der DSGVO. Die Kommission zog ein im Wesentlichen positives Fazit, da sich das Regelwerk überwiegend bewährt habe und weil den Belangen des Datenschutzes mehr Rechnung getragen würde als zuvor. Etwa 70 Prozent der

Europäer*innen sei die DSGVO bekannt und hätten die in der Verordnung enthaltenen Rechte ausgeübt. Allerdings sieht die Kommission auch Handlungsbedarf: Der Europäische Datenschutzausschuss (EDSA) der Aufsichtsbehörden müsse noch aktiver bei der einheitlichen Durchsetzung der Verordnung und die aufsichtsbehördliche Zusammenarbeit und Kohärenz gestärkt werden.

Die Umsetzung der DSGVO im NDR und seinen Beteiligungsunternehmen, den Gemeinschaftsunternehmen und Gemeinschaftseinrichtungen kann ebenfalls als gelungen angesehen werden. Die in den Jahren 2017 und 2018 eingeführten Strukturen, die Erklärungen, Informationen, Instrumente und Dokumentationspflichten funktionieren grundsätzlich.

Noch nicht abgeschlossen und umfänglich berücksichtigt wird allerdings das sogenannte **Verfahrensverzeichnis nach Art. 30 DSGVO**. Hiernach hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten mit diesen Inhalten zu führen:

- den Namen und die Kontaktdaten des Verantwortlichen
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Zwar wurde zur Erfüllung dieser Voraussetzung ein entsprechendes Muster bereitgestellt und ein Verfahren zur Dokumentation verabredet. Es hat sich jedoch wiederholt gezeigt, dass dies nicht hinreichend bekannt ist und eingesetzt wird. Im Jahr 2021 ist beabsichtigt, auf diese Sache einzugehen.

Insgesamt sei jedoch bezüglich des Zuständigkeitsbereichs des Rundfunkdatenschutzbeauftragten des NDR festgehalten, dass derzeit sowohl die Regulierung als auch die spezifische Umsetzung als gelungen bewertet werden kann.

2. Programm und Programmverbreitung

Datenschutzrechtliche Fragen und Probleme stellen sich hinsichtlich des Programms und seiner Verbreitung in unterschiedlichen Konstellationen. Folgende können unterschieden werden:

a) Datenschutzerklärungen und Informationspflichten

Die Überarbeitung der im Jahr 2018 zum Zeitpunkt des endgültigen Inkrafttretens der DSGVO novellierten Datenschutzerklärungen der vom NDR verantworteten Telemedienangebote (insbesondere ndr.de und tagesschau.de einschließlich der HbbTV-App der tagesschau, der ARD Quiz App sowie weiteren spezifischen Angeboten wie z. B. dem NDR Text in HbbTV, interne Foren) löst fortdauernden Beratungsbedarf aus. Im Jahr 2020 konnten die Anregungen aus der „**Untersuchung der Umsetzung der Datenschutzgrundverordnung (DSGVO) durch Online-Dienste**“ im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz aufgriffen und umgesetzt werden. Die Studie, zu finden unter

(https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/112919_DSGVO_Studie.pdf;jsessionid=6E5A2C2B0966725148776E30F8466427.2_cid324?__blob=publicationFile&v=2),

hatte mehr Transparenz und noch umfangreichere Darlegungen angeregt. Unabhängig davon hat der NDR Datenübertragungen in den Blick genommen, die durch die Nutzung vom Messenger-Diensten und Drittplattformen entstehen. Die Ausführungen in den Datenschutzerklärungen sind dadurch erweitert und vertieft worden.

b) Datenschutz für Kinder

Im Jahr Im Jahr 2018 wurde eine Erläuterung zum Datenschutz in Leichter Sprache veröffentlicht. Die Redaktion Barrierefreie Angebote und NDR Text des NDR hatte einen Text des Rundfunkdatenschutzbeauftragten in Leichte Sprache transkribiert und dafür eine Auszeichnung mit dem Leichte-Sprache-Preis der Universität Hildesheim und der Dudenredaktion erhalten. (https://www.ndr.de/fernsehen/service/leichte _sprache/Leichte-Sprache-Preis-fuer-NDR-Autor-Harenberg,leichtesprache432.html).

Datenschutz soll für alle verständlich und nachvollziehbar werden. Daher wurde im Berichtsjahr eine Erläuterung zum Datenschutz für Kinder verfasst, die die Kinderradioredaktion des NDR durch anschauliche Beispiele ergänzt und bereichert hat. Der Text ist dauerhaft im Internet abrufbar, z. B. unter file:///C:/Users/neuhoffh/Downloads/datenschutz704.pdf, und lautet wie folgt:

„Datenschutz verständlich erklärt: Hier wird für die Jüngsten erklärt, warum der Schutz von Daten im Internet so wichtig ist.

Was ist denn Datenschutz?

Andere Menschen wissen Dinge über Dich. Zum Beispiel wie Du aussiehst, wie Du heißt und was Du gerne magst. Auch Deine Schule weiß Einiges von Dir. Dein Geburtsdatum. Wie Deine Eltern heißen. Wo Du wohnst. Wann Du geboren bist. Diese Dinge heißen Daten.

Eigentlich sind das alles ganz persönliche Sachen. Und deshalb sind Deine Daten geschützt. Das heißt: Niemand darf Deine Daten ohne Grund benutzen oder ohne Erlaubnis weitersagen. Dafür gibt es ein Wort: **Datenschutz**.

Besonders wichtig ist der **Datenschutz**, damit mit Deinen Daten nichts Blödes passiert. Zum Beispiel können Leute mit Deinen Daten, ohne dass Du es willst, Geld verdienen.

Es gibt Firmen, die sammeln so begeistert Daten wie Eichhörnchen Nüsse sammeln.

Das machen die, weil sie dann genau wissen, ob sie Dir vielleicht Sachen verkaufen können, die zu Dir passen. Und wenn sie nichts zu verkaufen haben, was zu Dir passt, können sie aber anderen Firmen Deine Daten weitersagen.

Zum **Datenschutz** gibt es Regeln. An diese Regeln müssen sich alle Firmen in Europa halten.

Eine Firma muss Dich und Deine Eltern vorher fragen, wenn sie etwas mit Deinen Daten machen möchte. Zum Beispiel wenn die Firma Deine Daten an eine andere Firma weitergeben will. Du kannst mit Deinen Eltern auch eine Firma fragen, was sie mit Deinen Daten macht. Dann muss Dir die Firma das erklären.

Was macht der NDR mit Deinen Daten?

Auch der NDR ist eine Firma und muss sich an diese Regeln halten. Der NDR nimmt den Schutz Deiner Daten sehr ernst. Den Namen und den Wohnort von Menschen weiß der NDR zum Beispiel nur dann, wenn das wirklich nötig ist oder wenn jemand das dem NDR sagt.

Ein Beispiel: Wenn Du bei einer Radiosendung mitmachst und einen Buchpreis oder ein Spiel gewinnst, braucht der NDR natürlich Deine Anschrift, damit er Dir den Preis zuschicken kann. Sobald der Preis an Dich losgeschickt wurde, wird Deine Adresse gelöscht. Sie wird nicht aufbewahrt.

Niemals wird der NDR E-Mail-Adressen der Leute, die an den NDR schreiben, an Firmen oder Personen außerhalb des NDR weitergeben.

Wie ist das im Internet?

Wenn Du auf der Internetseite der Sesamstraße, von Mikado oder vom Ohrenbär ein Video guckst oder ein Spiel spielst, gilt ebenfalls der **Datenschutz**. Denn eine Internetseite funktioniert nur mit bestimmten Daten.

Das sind zum Beispiel das Datum und die Uhrzeit. Und eine IP-Adresse. Eine IP-Adresse ist so etwas wie der Name Deines Computers, Tablets oder Smartphones. Dieser Name Deines Computers wird oft Kennung genannt. Aber diese Daten haben keinen direkten Bezug zu Dir. Der NDR weiß also nicht, wer Du bist, wie Du aussiehst und wann Du spielst.

Der NDR weiß nur, wie oft ein Video gesehen oder ein Spiel gespielt wird und ob daher viele Menschen das Video oder das Spiel mögen. Er weiß aber nicht,

wer diese Menschen sind. An andere Firmen sagt der NDR das auch nicht weiter und löscht alles, wenn er das nicht mehr braucht.

Was ist ein Cookie?

Cookie ist ein englisches Wort. Auf deutsch heißt Cookie Keks! Aber jetzt geht es nicht um Kekse. Cookies sind nämlich auch kleine Dateien aus dem Internet. Cookies können ganz unterschiedliche Aufgaben haben. Einige Cookies sorgen dafür, dass Du eine Internetseite öffnen und ein Spiel spielen kannst. Andere Cookies zählen, wie viele Menschen ein Spiel gespielt haben.

Wenn Du eine Internetseite öffnest, dann wandern Cookies von einem Server über den Browser zu Deinem Computer. Ein Server ist so etwas wie eine große Rechenmaschine. Der Browser ist Dein Zugang zum Internet. Die Cookies kommen beim Surfen im Internet auf Deinen Computer.

Mit den Cookies ist das so eine Sache. Oft fragt Dich der Computer, ob Du Cookies „zulassen“ willst. Die Frage ist ein bisschen gemein: Wenn Du nicht zustimmst, geht es nämlich meistens nicht weiter und Du kommst nicht zu den Seiten, die Du erreichen willst. Wenn Du zustimmst, erlaubst Du, dass die Cookies in Deinen Computer reinkommen. Das kann in bestimmten Fällen blöd sein, weil manche Firmen Dich mit Hilfe der Cookies besser kennenlernen und Geld mit Deinen Daten verdienen wollen.

Einige Cookies sind wieder weg, wenn Du nicht mehr im Internet bist. Andere Cookies bleiben länger. Du kannst sie aber in den Einstellungen Deines Computers sofort wieder löschen. Es lohnt sich, in den Einstellungen Deines Computers zu gucken, was dort für Cookies sind. Denn einige sind notwendig, andere brauchst Du nicht und wieder andere sind nur neugierig und können weg. Am besten Du fragst einmal Deine Eltern danach!“

Die Veröffentlichung wurde beim Datenschutz Medienpreis DAME eingereicht. Mit diesem Preis werden Beiträge aller Art prämiert, die Datenschutz anschaulich und verständlich erklären und dabei zugleich die Themen und Sprache ihrer Zielgruppe treffen. Die Gewinner*innen stehen im April 2021 fest.

c) Anfragen zu den Angeboten und Datenschutzerklärungen des NDR

Knapp über 40 Anfragen, und damit deutlich mehr als im Jahr zuvor (2019: 15) wurden von den von Nutzer*innen, Hörer*innen und Zuschauer*innen des NDR zu den Programmangeboten des NDR und den Datenschutzerklärungen an den Rundfunkdatenschutzbeauftragten gerichtet. Dabei ging es um sehr unterschiedliche Belange, wie etwa

- Nachfragen und Hinweise zu den Datenschutzerklärungen und hier insbesondere zu Nutzungsmessungen und Befragungen
- Datenverarbeitungen im Falle des Abonnements von Push-Nachrichten und bei der Nutzung von Messenger-Diensten
- Löschbegehren im Falle der Teilnahme an Programmaktionen und Gewinnspielen
- Bestätigungen von Löschungen nach Beendigung von Programmaktionen
- Anfragen zu Ausschüttungen von Gewinnen
- Vorbringen zu Verletzungen des (eigenen oder auch fremden) Datenschutzrechts aufgrund der Verbreitung bestimmter Programminhalte
- Nachfragen zum Umgang mit personenbezogenen Daten bei Programmbeschwerden

Regelmäßig waren die Anfragen und Hinweise hilfreich und haben aufgezeigt, wie datenschutzrechtliche Belange noch deutlicher (z. B. in den Datenschutzerklärungen) vermittelt werden können. Die Prüfungen haben regelmäßig aber auch ergeben, dass Verletzungen des Rechts auf personelle Selbstbestimmung nicht vorlagen. Gleichwohl wurden von den zuständigen Redaktionen durch entsprechende Nachbearbeitung Änderungen von Beiträgen vorgenommen.

Beantwortet wurde auch der Fragenkatalog einer Universität im Rahmen der „Data Literacy Education“ (Interdisziplinäre Bildung für die digitale Wissensgesellschaft). Gestellt und beantwortet wurden Fragen zur Datenschutzerklärung der tagesschau App, zur Rolle und Bedeutung des Datenschutzes und

den Änderungen aufgrund der DSGVO, zum etwaigen Einsatz von sogenannten Privacy Icons und der Organisation des Datenschutzes im NDR.

d) Anfragen von Redaktionen

Datenschutzrechtlichen Beratungsbedarf haben auch Redaktionen an den Rundfunkdatenschutzbeauftragten herangetragen. In aller Regel geht es dabei um transparente und datensparsame Kontakte des NDR zu seinen Nutzer*innen, Hörer*innen und Zuschauer*innen, z. B. bei

- einer Aktion zu der tagesthemen-Serie #mittendrin in Deutschland
- bei der Gestaltung von datenschutzrechtlichen Hinweisen oder Anforderungen an Einwilligungserklärungen bei On- und Off-Air- Programmaktionen (bspw. bei einem Dating-Format oder zur Sendung „Treckerfahrer dürfen das!“)
- Voraussetzungen und Fristen der Speicherung von Teilnehmer*innen- und Gewinner*innendaten bei Gewinnspielen.

Regelmäßig werden auch organisatorische Fragen hinsichtlich des Zugriffs und der Sicherung sensibler Redaktionsdaten oder von Daten von Mitarbeitenden gestellt.

Der **Einsatz von Cookies** war ebenso Gegenstand der Beratungen, u. a. weil das entsprechende Urteil des Bundesgerichtshofs (Urteil vom 28. Mai 2020 – I ZR 7/16 -) nicht leicht lesbar ist. Insbesondere die Frage der Nutzungsmessung war zu erklären, wobei auf die einschlägige Veröffentlichung der RDSK Bezug genommen werden konnte:
„Der öffentlich-rechtliche Rundfunk verbreitet Telemedien, um seinen verfassungsrechtlichen Funktionsauftrag zu erfüllen. Nach der Rechtsprechung des Bundesverfassungsgerichts darf (und muss) er sein von den Beitragszahlern finanziertes Angebot im gesellschaftlichen Interesse auf allen publizistisch relevanten Plattformen zugänglich machen. Ob, wo und wie er damit seinen publizistischen Auftrag erfüllt, hängt von der Konfiguration dieses Angebots ab. Die Rundfunkanstalten sind dazu auf Erkenntnisse zur Akzeptanz und Nutzung ihres Angebots angewiesen. Dies gilt allerdings ausschließlich für ano-

nymisierte Auswertungen, wie sie auch im linearen Rundfunk üblich sind. Vergleichbar statistisch belastbare Methoden wie etwa die Messung der Zuschauerquote (Fernsehen) oder die Media-Analyse (Hörfunk) stehen dafür im Online-Bereich jedoch bislang nicht zur Verfügung. Die Rundfunkanstalten haben daher im Rahmen ihres verfassungsrechtlichen Funktionsauftrags ein berechtigtes Interesse am Einsatz von Cookies, die diese Aufgabe für ihr Onlineangebot übernehmen. Sie verfolgen damit kein (markt-)wirtschaftliches, sondern ein ausschließlich publizistisches Ziel.

Für die Rundfunkanstalten ist die anonymisierte Nutzungsmessung daher erforderlich, damit sie die ihnen durch Art. 5 Abs. 1 S. 2 GG übertragene Aufgabe optimal wahrnehmen können, Art. 6 Abs. 1 S. 1 lit. e) DSGVO. Auch nach Maßgabe einer Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO ist die Nutzungsmessung zulässig. Nach dem Urteil des EuGH vom 1.10.2019 kann das allgemeine Interesse des Verantwortlichen an einer Erfassung und Auswertung des Nutzungsverhaltens (insbesondere für die in § 15 Abs. 3 TMG genannten Zwecke) zwar nicht per se als „berechtigtes Interesse“ im Sinne von Art. 6 Abs. 1 S. 1 lit. f) DSGVO qualifiziert werden. Im Falle einer ausschließlich publizistisch motivierten anonymisierten Nutzungsmessung überwiegt jedoch das Interesse der Rundfunkanstalt (und der Gesamtheit ihres Publikums) ein etwa entgegenstehendes individuelles Interesse, Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

Anders stellt es sich hingegen bei den **Beteiligungsunternehmen des NDR** dar. Hier sind regelmäßig Einwilligungen von den Nutzer*innen einzuholen, sofern es sich nicht um sogenannte „funktionale Cookies“ handelt, also solche Cookies

- die dem Verantwortlichen eine (technische) Fehleranalyse ermöglichen,
- die der Sicherheit seines Angebots dienen,
- die Login-Daten der Nutzer*innen speichern,
- die für Transaktionen (Warenkorbfunktion) oder
- zur Individualisierung von Webseiteninhalten erforderlich sind.

Auf der Seite eines Tochterunternehmen war dies fast gelungen. Allerdings waren – und sind noch immer – Anpassungen vorzunehmen, weil mittels Nudging versucht wird, die Nutzer*innen zu wenig datenschutzfreundlichen Einstellungen zu bewegen. **Nudging ist das Vorspiegeln der Wahl der vermeintlich datenschutzfreundlichsten Variante durch farblich oder dunkel hinterlegte Felder, während tatsächlich Gegenteiliges geschieht**. Bei einem Tochterunternehmen des NDR durch ein dunkelblau hinterlegtes Feld suggeriert, die Nutzer*innen würden die für sie beste Wahl treffen, während dies tatsächlich aber nicht so ist. Daher war aufzugeben, dass die datenschutzrechtlichen Erfordernisse umgesetzt werden und zugleich vom Nudging abgesehen wird, damit den Nutzer*innen in einer fairen Weise die Möglichkeit geboten wird, die nur von ihnen gewählten Cookies zuzulassen.

e) Wegfall des Privacy Shields und Drittplattformen

Über die Neufassung der vom NDR verantworteten Datenschutzerklärungen wurde bereits berichtet. Zu untersuchen war in diesem Zusammenhang, wie sich bei der Nutzung von Drittplattformen, etwa bei Sprachassistenten, der Datenfluss verhält und die Verantwortlichkeiten (für die veranlasste Übertragung von Daten in die USA) darstellt.

Zu berücksichtigen war dabei auch, dass der EuGH im Juni 2018 entschieden hatte, dass ein Fanpage-Betreiber (bei Facebook) in der EU gemeinsam mit Facebook Ireland für die Datenverarbeitung grundsätzlich mitverantwortlich ist. Die Entscheidung ist auch für die Programmverbreitung auf anderen Drittplattformen einschlägig, wobei im jeweiligen Einzelfall die Verantwortung für die Datenverarbeitung gesondert zu beurteilen ist.

Das Gericht war zu dem Ergebnis gelangt, dass ein Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage ein für die Verarbeitung Verantwortlicher im datenschutzrechtlichen Sinne ist. Daher leistet auch der NDR einen kausalen Beitrag zur Verarbeitung personenbezogener Daten allein aufgrund der Präsenz auf Drittplattformen. Allerdings sind regelmäßig bei den vorgenommenen Programmverbreitungen Unterschiede zu verzeichnen,

so dass es sich nicht um eine gleichwertige Verantwortlichkeit bei den Plattformbetreibern und dem NDR handelt.

Entscheidend ist, wie sehr der NDR an der Erhebung und Weitergabe der Daten bei Drittplattformen mitwirkt oder davon profitiert. Im Ergebnis konnte festgehalten werden, dass es allenfalls ein unterschwelliges „Profitieren“ gibt, weshalb die Verantwortlichkeit gegen null tendiert, zumal die Nutzer*innen bei der Anmeldung auf der jeweiligen Plattform über die Datenverarbeitungen informiert werden und diesen dort zustimmen müssen. Diesbezüglich ist aber eine dauerhafte Beobachtung der Entwicklung der Plattformen notwendig. Die aktualisierten Datenschutzerklärungen gehen auf diese Umstände ein:

„Was Sie mit Sprachassistenten kommunizieren, wird von Ihrem Gerät aufgezeichnet und als Audiodatei in einer Cloud gespeichert. Auch bei der Nutzung der weiteren Plattformen und Dienste ist nicht auszuschließen, dass ein Transfer von personenbezogenen Daten auch in die USA erfolgt, da diese Anbieter Daten auf dortigen Servern speichern. Das Datenschutzniveau ist in den USA nach den Feststellungen des EUGH in der Entscheidung zum Privacy-Shield (Urteil in der Rechtssache C-311/18 „Schrems II“) geringer als im Geltungsbereich der DSGVO. Der NDR überträgt aber keine personenbezogenen Daten von Ihnen oder veranlasst eine solche Übertragung, da Sie regelmäßig aufgrund Ihrer Anmeldung oder Registrierung bei den Dienstanbietern einer entsprechenden Datenverarbeitung durch diese zugestimmt haben.“

3. Rundfunkteilnehmerdatenschutz

Die Überwachung des Rundfunkteilnehmerdatenschutzes ist eine regelmäßige Aufgabe. Datenschutzverletzungen oder besondere Vorfälle bezüglich des Rundfunkbeitragseinzugs beim Beitragsservice hat es nicht gegeben.

Einvernehmlich geklärt werden konnte mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, dass einem Anliegen einer Vollstreckungsbehörde des Landes Schleswig-Holstein nicht entsprochen werden kann: Die Vollstreckungsbehörde begehrte vom NDR **Informationen zu Vollstreckungsschuld-**

ner*innen, die über das gesetzliche geforderte Maß hinausgehen. Der NDR lässt bestandskräftige Rundfunkbeitragsforderungen durch die Vollstreckungsbehörden des Landes Schleswig-Holstein vollstrecken. Dazu teilt der NDR der zuständigen Vollstreckungsbehörde die Schuldner*innen, die zu vollstreckenden Forderungen und die Tatsache des Vorliegens eines Vollstreckungstitels mit. Die darüber hinaus begehrten Informationen, die auf mögliche Gefährdungen des Personals der Vollstreckungsbehörden hinweisen könnten, sind zum einen dem NDR nicht bekannt, insbesondere fehlt es aber auch an einer Rechtsgrundlage für die Übermittlung weiterer Datenkategorien.

Im Jahr 2019 hatten sich 8151 Personen an den Beitragsservice gewandt und um Auskunft ersucht. Für den NDR wurden 1245 Beauskunftungen erteilt. Für das Jahr 2020 ist ein signifikanter Anstieg zu verzeichnen: **33.379 Auskünfte wurden insgesamt erteilt, davon 4.997 für den NDR**. An den NDR in Hamburg haben sich 35 Personen gewandt. 3 Anfragen konnten nicht beantwortet werden, weil trotz entsprechender Aufforderungen keine hinreichende Identifizierung erfolgte.

Die Anzahl der Anfragen, Beanstandungen und Beschwerden, die an den Rundfunkdatenschutzbeauftragten gerichtet wurden, betrug 28 Zuschriften (mehrfache Eingaben im Falle der Personenidentität wurden nicht gezählt). Wie in den Jahren zuvor auch, liegt der Schwerpunkt der Anfragen, Beanstandungen und Beschwerden im Bereich des Rundfunkbeitragseinzug und in einer vorgetragenen „falschen“ Datenverarbeitung. Datenschutzverletzungen waren in der Regel allerdings nicht erkennbar, weil die Datenverarbeitung zum Zwecke des Rundfunkbeitragseinzugs der Beitragspflicht folgt und Löschbegehren daher im Fall einer solchen Pflicht ins Leere gehen.

4. Beschäftigtendatenschutz

Fragen des Beschäftigtendatenschutz stellten sich überwiegend im pandemischen Gewand.

a) Kollaborationssysteme

Der Einsatz elektronischer Anwendungen und Plattformen, die eine nicht ortsgebundene Kommunikation und Zusammenarbeit ermöglichen – sogenannte Kollaborationssysteme –, hatte aufgrund der pandemischen Umstände einen erheblichen Zulauf erfahren. Dienstreisen wurden maßgeblich durch Videokonferenzen ersetzt und in der zweiten Märzhälfte 2020 arbeiteten bereits rund 2000 Mitarbeiter*innen des NDR vom Homeoffice aus. Aufgrund der stark gestiegenen **Nachfrage nach Videokonferenzen** kam es temporär zur Überlastungen des ARD-Konferenzsystems. Zugleich wurden redaktionell erforderliche Informationen von Dritten ebenfalls videobasiert kommuniziert, so dass datenschutzrechtliche Fragen der aktiven und passiven Nutzung von Konferenzsystemen das Berichtsjahr begleiteten (und dieses auch überdauern werden).

Bei manchen prominenten Systemen gab und gibt es hinsichtlich des Datenschutzes und IT-Sicherheit Bedenken, in Teilen auch bezüglich der passiven Nutzung. Es war daher darauf hinzuweisen, dass die jeweils in der Rundfunkanstalt freigegebenen Dienste vorrangig zu nutzen sind. Für den Fall der Zugänglichkeit redaktionell notwendiger Informationen über ausschließlich andere Systeme, war und ist im Einzelfall eine Nutzung von Systemen Dritter möglich. Diesbezüglich wurden nach datenschutzrechtlichen und IT-sicherheitsrechtlichen Maßgaben entsprechende Anforderungen formuliert.

b) Einsatz der Corona-Warn-App

Am 16. Juni 2020 wurde die „Contact-Tracing-App“ oder auch „Corona-Warn-App“ zur Verfügung gestellt. Ziel der Anwendung ist, Kontakte von infizierten Personen rasch zu ermitteln und nachzuverfolgen, um die Verbreitung des Virus einzudämmen.

Das Robert-Koch-Institut (RKI) ist Anbieter dieser App. Die Nutzung ist freiwillig. Daher muss im Falle einer Nutzung nach dem erstmaligen Aufruf der App gegenüber dem RKI durch Antippen des Buttons „Risiko-Ermittlung aktivie-

ren“ zugestimmt werden, dass die App im Rahmen der Risiko-Ermittlung personenbezogene Daten verarbeiten darf.

Nach Angaben des RKI wurde die App so konzipiert, dass möglichst wenig personenbezogene Daten verarbeitet werden. Die App soll danach keine Daten erheben, „die es dem RKI oder anderen Nutzern ermöglichen, auf Ihre Identität, Ihren Gesundheitsstatus oder Ihren Standort zu schließen. Zudem verzichtet die App bewusst auf jegliche Erfassung oder Analyse Ihres Nutzungsverhaltens durch Tracking-Tools.“ Einzelheiten über die Verarbeitung von personenbezogenen Daten hatte das RKI in einer Datenschutzerklärung für die Corona-Warn-App in einem Dokument zusammengestellt (https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf).

Es wurde die Frage an den Rundfunkdatenschutzbeauftragten herangetragen, ob auch eine **verpflichtende Installation der App** – zumindest auf Geräten des NDR – möglich ist. Ergebnis der im NDR veröffentlichten Prüfung war, dass die Freiwilligkeit der Nutzung und die damit einhergehende Einwilligung der jeweils nutzenden Person im Arbeitsumfeld bestehen bleibt. Damit die Freiwilligkeit gewährleistet ist, darf es keine Verpflichtung für Beschäftigte geben, die Corona-Warn-App auf privaten oder dienstlichen NDR–Geräten zu nutzen. So darf beispielsweise die Rückkehr aus dem Homeoffice ins Büro nicht mit der Nutzung der App verknüpft werden, auch gibt es keine Verpflichtung, dienstliche Smartphones außerhalb der Arbeitszeiten mit sich zu führen. Zusammenfassend gilt daher, dass eine Nutzung der App auf dienstlichen Geräten des NDR möglich ist, dies aber nur wenn die*der Geräteinhaber*in sich freiwillig dafür entscheidet. Weiterhin besteht auch **kein Anspruch des Arbeitsgebers** darauf, sich Zugang zu den Mitteilungen in der App zu verschaffen und zu kontrollieren, ob eine nutzende Person Warnungen erhalten hat.

Aus datenschutzrechtlicher Sicht gibt es insgesamt keine Bedenken gegen eine freiwillige Nutzung der Corona-Warn-App, die Freiwilligkeit muss aber auch tatsächlich gewährleistet sein.

c) Umgang mit Corona-Tests und Testergebnissen

Die andauernde Pandemie und die im Laufe des Berichtsjahres immer stetig steigenden Infektionszahlen warfen eine Reihe von Fragen im Umgang mit (vermeintlich) infizierten Personen im NDR auf.

Es wurde daher beispielsweise erfragt, ob der NDR den Beschäftigten mitteilen kann, dass eine beschäftigte Person am Virus erkrankt ist, auch unter Nennung des konkreten Namens. Da die Kenntnis von der Corona-Erkrankung einer/s Beschäftigten für diese Person zu einer Stigmatisierung führen kann, war darauf zu weisen, dass die Meldeketten grundsätzlich den Vorgaben der Gesundheitsbehörden folgen, entsprechend dem Grad der Kontakte, die die infizierte Person aufgrund gesetzlicher Vorgaben mitteilen muss (https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Kontaktperson/Management.html). Soweit möglich, war und ist daher die Nennung des Namens der/des Betroffenen grundsätzlich zu vermeiden. Gleichzeitig sind Personen, welche in direktem Kontakt mit einem Infizierten waren, zu warnen (und werden in der Regel selbst zur Eindämmung der Ansteckungsgefahr von der Arbeit freigestellt). Regelmäßig kann eine derartige Maßnahme abteilungs- bzw. teambezogen ohne konkrete Namensnennung erfolgen. Ausnahmsweise unter Abwägung der Umstände des konkreten Falls muss der NDR Kontakt mit den Gesundheitsbehörden aufnehmen und um deren Entscheidung ersuchen. Ist auch dies nicht möglich, dürfen auch die übrigen Mitarbeiter*innen über den Verdacht der Ansteckung oder der Erkrankung der konkreten Person informiert werden, um Infektionsquellen zu lokalisieren und einzudämmen. Soweit möglich, ist also die **Identität von positiv auf Covid-19 getesteten Personen vertraulich** zu behandeln und bei etwaigen Informationen der Empfängerkreis klein zu halten. Bei Beschäftigten, die einen unmittelbaren Kontakt zu einer infizierten Personen hatten, kann die zielgerichtete Offenlegung der Identität erforderlich sein. Das können Fälle z. B. sein, in denen ein Büro geteilt wird. Die Zulässigkeit folgt dann aus § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b DSGVO.

Weiterhin wurde zwecks Ermittlung von Kontaktpersonen das vertrauliche Führen eines Kontakttagebuchs empfohlen.

Auch die Frage, ob der NDR einen Corona-Test verlangen oder anordnen kann, wurde wiederholt gestellt. Hier gilt, dass Beschäftigte grundsätzlich nicht verpflichtet sind, dem Arbeitgeber Diagnosen oder Krankheitssymptome zu offenbaren. Auch wenn das Interesse nachvollziehbar ist, herauszufinden welche Beschäftigten zu einer Risikogruppe gehören und damit besonderer Schutzmaßnahmen bedürfen, rechtfertigt dies keine Erhebung von Gesundheitsdaten. Es bleibt dabei, dass der Arbeitgeber die Preisgabe sensibler Gesundheitsdaten über spezifische Anfälligkeiten grundsätzlich nicht verlangen kann. Unternehmen ist es **grundsätzlich nicht erlaubt**, seine **Beschäftigten zu einem Corona-Test zu verpflichten**. Nur die Gesundheitsbehörden können dies aufgrund entsprechender gesetzlicher Verpflichtungen. Auch die Vorlage eines freiwilligen oder von einer Gesundheitsbehörde angeordneten Testergebnisses kann ein Arbeitgeber von Beschäftigten nicht verlangen. Tests einzelner Personen oder von Beschäftigten bestimmter Bereiche dürfen mangels Rechtsgrundlage nur durchgeführt werden, wenn die Betroffenen sich freiwillig damit einverstanden erklären. Dafür sind ausdrückliche, eindeutige und ohne Zwang abgegebene Einwilligungserklärungen notwendig. Der Arbeitgeber muss zudem nachweisen können, dass entsprechende Einwilligungserklärungen eingeholt wurden. Ebenfalls von Bedeutung war, dass Testergebnisse nur entweder der jeweils betroffenen Person oder der Betriebsärztin ausgehändigt werden dürfen, sofern keine anderslautenden Einverständniserklärungen abgegeben wurden.

d) Homeoffice

Wie bereits erwähnt, konnte frühzeitig eine Vielzahl von Beschäftigten des NDR im Homeoffice ihre Tätigkeit zu verrichten. Entsprechende Beratungen zum Einsatz von Dienstmitteln aus datenschutzrechtlicher Sicht wurden vom Rundfunkdatenschutzbeauftragten geleistet. Gleiches galt auch bezüglich einer **Dienstvereinbarung zum Homeoffice**, die im Berichtsjahr allerdings nicht mehr in Kraft trat. Zwischen dem NDR und dem Rundfunkdatenschutzbeauftragten besteht Einvernehmen, dass eine solche Vereinbarung folgende Regelungsinhalte beinhalten muss:

- Die Regelungen des NDR zum Datenschutz und zur IT-Sicherheit gelten auch für das regelmäßige und nicht regelmäßige mobile Arbeiten.
- Vertrauliche Daten, dienstliche Informationen und sonstige dienstliche Unterlagen sind stets und überall so zu schützen, dass diese nicht von unbefugten Dritten (einschließlich der Haushaltsangehörigen) eingesehen, genutzt oder entwendet werden können, gegebenenfalls durch das Ergreifen geeigneter technischer und organisatorischer Maßnahmen. Dazu zählen auch ein besonders sorgsamer Umgang ist mit Passwörtern und weiteren Zugangsvorrichtungen zu Netzen, Mailsystemen und Endgeräten.
- Tätigkeiten, bei denen überwiegend besonders schützenswerte personenbezogene oder vergleichbar sensible Daten bearbeitet werden, sind grundsätzlich nur dann für das mobile Arbeiten geeignet, wenn die Verarbeitung den maßgeblichen gesetzlichen und betrieblichen Bestimmungen entspricht und die/der Rundfunkdatenschutzbeauftragte dem vorher zugestimmt hat.
- Soweit im Rahmen des mobilen Arbeitens personenbezogene Daten anfallen, werden sie nicht für eine Leistungs- und Verhaltenskontrolle verwendet.

e) Weitere Tätigkeiten im Zusammenhang mit der Corona-Pandemie

Weitere Anfragen im Zusammenhang mit der Corona-Pandemie betrafen

- eine Unternehmensweite Abfrage zum Thema „Arbeiten unter Corona-Bedingungen“,
- Vereinbarungen mit Dritten über die Durchführung von Maßnahmen zur Eindämmung der Pandemie,
- die Bearbeitung und Berechnung des monatlichen Corona-Minderungsgeldes für freie Mitarbeiter*innen sowie
- die Erarbeitung von datenschutzkonformen Kontakterfassungsbögen für Gäste in den Kantinen.

f) Akkreditierungen und Einlasserfordernisse

Die Beantwortung von datenschutzrechtliche Anfragen zu **Akkreditierungsaufforderungen** bei Sportveranstaltungen gehören zum Regelgeschäft und waren regelmäßig problematisch. Letztlich konnten aber auch große Verbände davon überzeugt werden, dass für Akkreditierungen

- der jeweilige Name der Mitarbeiter*in,
- ggf. ein Foto und
- die Anschrift des NDR (nicht die privaten Anschriften)

ausreichend sind. Aufgrund erforderlicher Hygienekonzepte der Veranstalter fielen die Anforderungen an die Zulassung zu Sportveranstaltungen im Jahr 2020 umfangreicher aus. Hier wurden regelmäßig Temperaturmessungen und das Ausfüllen von Gesundheitsfragebogen verlangt. Auch wenn die geprüften Hygienekonzepte den jeweiligen Corona-Verordnungen entsprachen, war darauf zu weisen, dass – die teils auch im NDR praktizierte – **Erhebung von Körpertemperaturen** eine Verarbeitung von personenbezogenen Daten darstellt, die besonders geschützt sind (Gesundheitsdaten). Ebenso wie Corona-Testergebnisse gehört die Körpertemperatur zu den besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO und ist damit besonders schutzwürdig. Daraus folgt, dass die Anforderungen, die an die Rechtmäßigkeit der Verarbeitung solcher Daten gestellt werden, erhöht sind. Zu Bedenken ist dabei auch, dass die bloße Tatsache, dass eine erhöhte Körpertemperatur zu verzeichnen ist, noch nicht den Schluss auf das Vorliegen einer Corona-Infektion zulässt (und umgekehrt muss eine bereits bestehende Infektion nicht zwangsläufig mit einer erhöhten Körpertemperatur einhergehen). Daher ist bereits an der Geeignetheit der Körpertemperaturmessung zu zweifeln. Zudem stehen einem Arbeitgeber andere Möglichkeiten zur Verfügung, seiner Fürsorgepflicht nachzukommen (Homeoffice etc.). Sofern eine Präsenz von Beschäftigten am Arbeitsplatz erforderlich ist, ist es vorzugswürdig darauf hinzuweisen, dass beim Verspüren/Verdacht von Symptomen ein Arzt aufzusuchen ist, um den Gesundheitszustand abklären zu lassen.

Da das Abfragen und/oder Erheben von Gesundheitsdaten einer erhöhten Rechtfertigung bedarf, ist dies nur mit entsprechenden Einwilligungen der betroffenen Personen möglich. Auch hier gilt also – wie im Falle etwaiger Corona-Tests: Beschäftigte müssen dafür eine ausdrückliche, eindeutige und ohne Zwang abgegebene Einwilligung erklären. Der Arbeitgeber muss zudem nachweisen können, dass entsprechende Einwilligungserklärungen eingeholt wurden. Lediglich in räumlichen Ausnahmefällen kann dies anders zu beurteilen sein, etwa bei besonders engem Kontakt. Dann können nicht die konkret erfragten Informationen wie Krankheitssymptome oder die Körpertemperatur vom Arbeitgeber erhoben und gespeichert werden, sondern die Information, dass aufgrund entsprechender Kontrolle die betroffene Person aufgefordert wurde, sich für einen definierten Zeitpunkt nicht an die Arbeitsstätte zu begeben.

g) Schulungen

Auch im Jahr 2020 wurden datenschutzrechtliche Schulungen durchgeführt. Stets werden diese für die neuen Auszubildenden im kaufmännischen und technischen Bereich angeboten und durchgeführt. Weiterhin gab es Schulungen für Mitarbeitende des NDR im Personal- und Produktionsbereich.

Schulungen dienen dazu, für datenschutzrechtliche Belange zu sensibilisieren, unabhängig davon welche Personen von einer Datenverarbeitung betroffen sind. Durch die Stärkung des Datenschutzniveaus soll zugleich erreicht werden, dass vom NDR nicht freigegebene IT-Anwendungen nicht genutzt werden, bzw. nur nach einem dafür im NDR etablierten Verfahren. Denn die Nutzung von IT-Systemen, Anwendungen und sonstigen Angeboten/Tools aus dem Internet ohne eine vorherige Prüfung birgt erhebliche Risiken für den NDR und jeden einzelnen Mitarbeitenden unabhängig davon, ob nur sie*er die*der Nutzende ist. Die **ungeprüfte und nicht vom NDR freigebende Nutzung** solcher Systeme kann mit dem Begriff „**Schatten-IT**“ beschrieben werden: Es sind also solche Systeme, die ohne Kenntnis der zuständigen Fachabteilung des NDR, der IT-Sicherheit und des Datenschutzes zum Einsatz gebracht werden. Während die IT-Sicherheit maßgeblich den Schutz der Informationssysteme des NDR im Blick hat, richtet sich das Augenmerk des Datenschutzes auf den

Schutz von personenbezogenen Daten von Beschäftigten und Dritten. Systeme, die vor dem Einsatz im NDR nicht hinreichend geprüft worden sind, können – in vielen Fällen von den Anwendenden unbemerkt – Daten von (mobilen oder stationären) Computern oder aus den Netzen des NDR abgreifen, diese manipulieren und für unerwünschte, manchmal auch kriminelle Zwecke genutzt werden.

Aus diesem Grund hatte der **Rundfunkdatenschutzbeauftragte des NDR wiederholt angeregt**, ein **Schulungskonzept** aufzusetzen, mit dem die regelmäßig gemeinsam vom IT-Sicherheitsbeauftragten und Rundfunkdatenschutzbeauftragten durchgeführten Schulungsveranstaltungen erweitert werden, um konkrete Informationen und Handlungsanweisungen aus den spezifischen Fachbereichen, so dass die wesentlichen Belange

- Was ist, was will die IT-Sicherheit? Was haben Beschäftigte zu beachten?
- Was ist, was will der Datenschutz? Was haben Beschäftigte zu beachten?
- Was bietet der NDR? Wo finde ich technische Anwendungen, wer sind die Ansprechpartner*innen? Was muss ich tun, um neue Anwendungen/Tools in Einsatz zu bringen?

gebündelt behandelt werden können.

Überdies wurde angeregt, durch geeignete Veröffentlichungen die wesentlichen Arbeitsmittel zur Bewältigung der dienstlichen Anforderungen besser bekannt zu machen. Die Anregungen wurden allerdings nur rudimentär aufgegriffen bzw. bis auf Weiteres zurückgestellt.

h) Datenverarbeitung in Personalvertretungen des NDR

Letztlich doch noch einvernehmlich und eine aufsichtsrechtliche Maßnahme abwendend, konnte die Datenverarbeitung in Personalvertretungen des NDR geregelt werden. Dem Rundfunkdatenschutzbeauftragten wurde bereits im Jahr 2019 die Frage vorgelegt, an welchen Fristen sich die **Speicherung von Personaldaten bei den Personalvertretungen** zu orientieren habe. Mangels

vorhandener Regelungen wurde ein Vorschlag unterbreitet, der sich an entsprechenden Vorgaben der Landespersonalvertretungsgesetze orientiert:

- Unterlagen mit personenbezogenen Daten, die anlässlich eines Mitbestimmungsverfahrens zur Verfügung gestellt wurden, sind nach dessen Abschluss zurückzugeben oder zu löschen. Ihre Sammlung, fortlaufende aktenmäßige Auswertung sowie die Speicherung und elektronische Auswertung der in ihnen enthaltenen Daten in Dateien durch den Personalrat ist unzulässig.
- Unterlagen des Personalrats, die personenbezogene Daten enthalten (zum Beispiel Niederschriften, Personallisten), sind vor unbefugter Einsichtnahme zu schützen, aufzubewahren und spätestens nach Ablauf einer weiteren Amtsperiode des Personalrates zu vernichten.
- Maximal sind Vorgänge über die Beteiligung von Personalräten nicht länger als 1 Jahr, nachdem die Angelegenheit in der Personalratssitzung behandelt wurde, aufzubewahren. Diese Frist gilt auch für Sitzungsniederschriften des Personalrats, hier aber bezogen auf den Ablauf der Amtszeit des Gremiums.

Die gegen diese Speicherfristen vorgebrachten Einwände konnten nicht überzeugen, so dass schließlich dem Rundfunkdatenschutzbeauftragten bestätigt wurde, nach diesen Vorgaben zu verfahren und ältere Unterlagen zu vernichten/löschen.

Weitere Tätigkeiten – auch mit Bezug zum Beschäftigtendatenschutz – waren beispielsweise die Überarbeitung einer EDV-Rahmendienstvereinbarung, Anfragen zu E-Mail-Verteilern und Zugriffsberechtigungen und zu weiteren Projekten und Vorhaben des NDR, die im Folgenden aufgeführt sind.

5. Weitere Tätigkeitsschwerpunkte im NDR

Digitalisierungs-, Organisations- und Strukturprozesse sind alltäglich und zahlreich. Aspekte des Datenschutzes sind immer zu berücksichtigen. Die Anzahl der im NDR „technischen“ Projekte beträgt weit über 100 und betrifft diverse Bereiche des NDR.

a) Organisations- und Strukturprojekte

Datenschutzrechtliche Aspekte waren – auszugsweise – zu begutachten bei

- Bildaufnahmen von Beschäftigten zur Dokumentation von Baufortschritten
- Systemen zum Kundenbeziehungsmanagement
- dem Einsatz von Cloudanwendungen
- dem Ausbau von Kameraüberwachung
- der Ausstattung crossmedialer Arbeitsplätze
- der Errichtung eines crossmedialen Nachrichtenhauses
- der Erneuerung von Studios
- Systemen zur Bedrohungsanalyse von Daten
- Plattformen für das kollegiale Wissensmanagement (Wikis)
- dem Rollout von Windows 10
- einem gemeinsamen, zentralen ServiceDesk der Rundfunkanstalten
- Personalkonzepten
- Einstellungstests
- Systemen zur Produktivzeiterfassung

Hinzu kamen über 100 Prüfungen von kleineren Softwareanwendungen, Apps und sonstigen digitalen Anwendungen.

b) Datenübermittlungen in Drittländer

Das bereits erläuterte Urteil des EuGH zum Wegfall des EU-US-Privacy-Shields war zum Anlass zu nehmen, um eine Übersicht aller Bereiche des NDR zu erbeten, aus der hervorgeht, welche Übermittlungen personenbezogener Daten in die USA der NDR vornimmt oder veranlasst. Die abschließende Prüfung geeigneter Maßnahmen war im Berichtsjahr noch nicht abgeschlossen, weil es sich um eine Vielzahl von Systemen handelt und das Ergreifen entsprechender Maßnahmen nicht trivial ist.

Zum 31.01.2020 war Großbritannien aus der EU ausgetreten. Obwohl Großbritannien damit ab dem 01.02.2020 zu einem Drittland im datenschutzrechtlichen Sinne geworden war, konnten personenbezogene Daten bis zum 31.12.2020 weiterhin ohne besondere Schutzmaßnahmen nach Großbritannien übermittelt werden. Denn das Austrittsabkommen zwischen der EU und Großbritannien legte fest, dass die DSGVO in einem Übergangszeitraum bis zum 31.12.2020 weiterhin auch in Großbritannien gilt. In der gemeinsamen politischen Erklärung zum zukünftigen Verhältnis zwischen der EU und Großbritannien wurde zudem vereinbart, dass die EU-Kommission bis zum Ende des Übergangszeitraumes Angemessenheitsbeschlüsse erlässt. Bis kurz vor Ende des Jahres 2020 lagen keine Angemessenheitsbeschlüsse vor und der Übergangszeitraum wurde bis Mitte Dezember nicht verlängert. Es waren daher Vorbereitungen getroffen worden, um Datentransfers mit den besonderen Maßnahmen nach Kapitel V der DSGVO abzusichern. Sehr kurzfristig stellte sich jedoch heraus, dass in dem Brexit-Deal Übermittlungen personenbezogener Daten von der EU in das Vereinigte Königreich Großbritannien und Nordirland für eine Übergangsperiode nicht als Übermittlungen in ein Drittland (Art. 44 DSGVO) angesehen werden sollen. Diese Periode beginnt mit dem In-Kraft-Treten des Abkommens und endet, wenn die EU-Kommission das Vereinigte Königreich betreffende Adäquanzentscheidungen nach Art. 45 Abs. 3 DSGVO und Art. 36 Abs. 3 Richtlinie (EU) 2016/680 getroffen hat, spätestens jedoch nach vier Monaten. Dieses Enddatum kann um zwei Monate verlängert werden, falls keine der beteiligten Parteien widerspricht. Der angenommene Handlungsbedarf und die entsprechenden Vorkehrungen blieben daher – jedenfalls zunächst – ohne praktische Relevanz.

c) Kommunikation und Kollaboration

Eine Reihe von Fragen, wie im NDR und mit Externen kommuniziert und zusammengearbeitet wird, war im Jahr 2020 noch offen. Die grundlegenden und gängigen Formen der Kommunikation können derzeit datenschutzkonform abgewickelt werden:

- **Telefonie**

  Weitgehend unproblematisch aus datenschutzrechtlicher Sicht stellt sich derzeit die Telefonie dar. Ob dies zukünftig so bleiben wird, nämlich wenn die Nutzung von Telefondienstleistungen aus der Cloud als Ersatz oder in Ergänzung lokaler Telefonanlagen vorgenommen wird, muss datenschutzrechtlich weiter begleitet werden.

- **E-Mails**

  Ebenfalls weitgehend unproblematisch stellt sich die E-Mail-Nutzung dar. Allerdings muss über den Einsatz wirksamer Verschlüsselungstechniken nachgedacht werden.

- **Telefon- und Videokonferenzen**

  Während andere Systeme mit großem Aufwand zusammengeführt und harmonisiert werden, steht das ARD-Konferenzsystem vor dem Aus. Derzeit ist eine Abschaltung zum Ende des Jahres 2021 geplant. Dies ist aus datenschutzrechtlicher Sicht misslich. Im Berichtsjahr war noch kein Ersatz gefunden.

- **Terminabsprachen**

  Für Terminabstimmungen und Umfragen steht ein Tool von ARD und ZDF bereit. Datenschutzrechtlich ist dies zu begrüßen.

- **Messengerdienste**

  Die Frage, mit welchem Messengerdienst zukünftig im NDR gearbeitet werden soll, war im Berichtsjahr noch nicht beantwortet. Die derzeit eingesetzten Dienste erfüllen datenschutzrechtliche Anforderungen überwiegend.

- **Datei- und Informationsaustauschservice**

  Ein entsprechendes Tool von ARD und ZDF steht bereit, mit dem große Dateien innerhalb und außerhalb der Rundfunkanstalten über das Internet ausgetauscht werden können. Datenschutzrechtlich ist dies zu begrüßen.

- **Automatische Spracherkennung**

  Ebenfalls steht ein datenschutzkonformes System zur Verfügung, mit der das gesprochene Wort in ein Text umgewandelt wird.

Alternative und ergänzende Anwendungen waren im Berichtsjahr immer wieder Gegenstand von datenschutzrechtlichen Anfragen und Bewertungen, so etwa

- diverse Tools, mit dem Wahlen und Abstimmungen durchgeführt werden können,
- Business-Messenger,
- sogenannte Boards zum gemeinsamen Diskutieren und Erarbeiten von Dokumenten und Konzepten.

Entscheidungen über den Einsatz wurden vom NDR noch nicht getroffen.

d) Datensicherheit

Nicht zuletzt waren immer wieder Fragen der Datensicherheit zu bearbeiten. So waren interne personenbezogene Daten des NDR zeitweise im Internet abrufbar. Dieses Datenleck wurde durch geeignete Maßnahmen geschlossen, auch der Meldepflicht an den Rundfunkdatenschutzbeauftragten wurde entsprochen. Durch das Datenleck wurde der Grundsatz der Integrität und Vertraulichkeit von personenbezogenen Daten verletzt, denn personenbezogene Daten sind so zu verarbeiten, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist. Da Unbefugte Zugang zu den Daten erlangen konnten, war wegen der Verletzung der genannten Grundsätze der Datenverarbeitung eine Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO auszusprechen. Weiterhin kommt es auch immer wieder vor, dass in Beiträgen – beispielsweise durch das Abfilmen von Bildschirmen – Links oder Daten (Handynummern, Passworte) sichtbar werden, so dass auf gesteigerte Sorgfalt hinzuweisen ist.

Fortwährend sind Maßnahmen zur Anhebung der IT-Sicherheit – und damit auch der Datensicherheit – zu begleiten. Zu diesem Zweck wurde etwa die Kennzeichnung externer E-Mails eingeführt, um die Achtsamkeit für externe E-Mails zu erhöhen, die Schadsoftware enthalten können. Weiterhin lädt der NDR nunmehr externe Fachkundige ein, im Rahmen der Rechtsordnung wohlmeinende und schadlose Untersuchungen von Sicherheitslücken durchzuführen („ethical security researches done in security vulnerabilities“).

F. Fazit

Das Berichtsjahr 2020 hat für den NDR zwar nicht unbedingt einen Digitalisierungsschub gebracht, aber sicherlich die Nutzung digitaler Systeme intensiviert und die Nachfrage nach weiteren Mitteln der Zusammenarbeit erhöht. Dass Digitalisierung und Datenschutz untrennbar miteinander verbunden sind, wurde eingangs erläutert. Der Bedarf an datenschutzrechtlichen Anfragen und Beratungen wächst somit kontinuierlich und wird voraussichtlich weiterhin im Schwerpunkt Strukturprozesse und Kollaborationsanwendungen betreffen. Zugleich scheint sich eine strenge Rechtsprechung bezüglich des Datenschutzes zu etablieren, was zu begrüßen ist. Grundsätzlich ist ein reflektierter Umgang mit personenbezogenen Daten zu erkennen, auch wenn mancherorts vorschnell der Gebrauchstauglichkeit und Benutzerfreundlichkeit Vorzug gegeben wird. Es bleibt daher eine dauerhafte, spannende und herausfordernde Aufgabe, die Belange des Datenschutzes durchzusetzen.