NORDDEUTSCHER RUNDFUNK

Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten des NDR

für das Berichtsjahr 2021

Dr. Heiko Neuhoff

Hamburg im Januar 2022

© Alex – Fotolia

Vorgelegt wird hiermit der Bericht gemäß § 46 Abs. 4 NDR Staatsvertrag i. V. m. Art. 59 DSGVO über die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR im Jahr 2021.

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 Struktur des Tätigkeitsberichts für das Jahr 2021 folgt der des vorherigen Jahres. Gründe dafür sind u. a. wohlwollende Rückmeldungen zum Aufbau der Darstellung und ein möglichst schneller Zugriff auf die Inhalte. Der Verfasser des Berichts ist aus dem zuletzt genannten Grund überdies bemüht, die Tätigkeiten möglichst straff und verständlich darzulegen. Dies fällt nicht immer leicht. Denn: Die zu prüfenden Anfragen und die aufzuklärenden Sachverhalte werden stetig umfangreicher und komplexer.

Das Jahr 2021 war aus Sicht des Datenschutzes u. a. maßgeblich dadurch gekennzeichnet, dass

- vermehrt Cloud-Dienste genutzt werden,
- die Vorhaltung von Daten mehr und mehr ausgelagert, also Dritten übertragen wird, und
- die Sicherheit von Daten stärker in den Fokus geriet.

Ganz grundsätzlich besteht die Tätigkeit aus

- Beratungen bei Datenverarbeitungsvorgängen unterschiedlichen Umfangs,
- der Überwachung und Durchsetzung datenschutzrechtlicher Vorgaben,
- der Prüfung von externen und internen Anfragen und Beschwerden und
- dem Austausch und der Zusammenarbeit mit anderen Aufsichtsbehörden und Datenschutzbeauftragen.

B. Rechtsgrundlagen der Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR

Materiell-rechtlich blieben die Grundlagen für die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR unverändert. Maßgeblich ist weiterhin die seit dem 25. Mai 2018 anwendbare Datenschutzgrundverordnung (DSGVO). Seit dem 1. September 2021 sind die Regelungen des NDR-Datenschutz-Staatsvertrags in den neu gefassten NDR Staatsvertrag integriert. Der Regelungsgehalt hat sich dabei nicht geändert. Die Vorschriften finden sich nun wortgleich in den §§ 43 bis 46 NDR Staatsvertrag. Der Rundfunkdatenschutzbeauftragte ist danach Aufsichtsbehörde nach Art. 51 DSGVO und überwacht die Einhaltung der Daten-

schutzvorschriften bei der gesamten Tätigkeit des NDR und seiner Beteiligungsunternehmen im Sinne des § 16 c Abs. 3 Satz 1 RStV.

Mit dem neuen NDR Staatsvertrag ist zudem der Aufgabenbereich des Rundfunkdatenschutzbeauftragten erweitert worden. Mit der Einführung eines Informationsfreiheitsanspruches gegen den NDR (§ 47 NDR Staatsvertrag) ist der Rundfunkdatenschutzbeauftragte Beschwerdestelle geworden, vergleichbar mit den Beauftragten für die Informationsfreiheit der Länder bzw. des Bundes. Die Ländergesetze sehen regelmäßig vor, dass die Beauftragten für die Informationsfreiheit Anlaufstelle sind für Personen, die der Ansicht sind, „dass ihrem Anspruch auf Information nicht hinlänglich nachgekommen wurde oder dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von einer auskunftspflichtigen Stelle eine unzulängliche Antwort erhalten hat“ (§ 14 Hamburgisches Transparenzgesetz). Entsprechendes gilt für antragstellende Personen, die Informationen vom NDR begehren. Der neu geschaffene § 47 Abs. 11 NDR Staatsvertrag lautet:

„Antragstellende, die der Ansicht sind, dass der Informationsanspruch zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass nur eine unzulängliche Antwort gegeben worden ist, können den Rundfunkdatenschutzbeauftragten oder die Rundfunkdatenschutzbeauftragte des NDR anrufen.“

Alle wesentlichen Rechtsgrundlagen und Ausführungen dazu sind abrufbar auf der neu gestalteten Internetseite des Rundfunkdatenschutzbeauftragten des NDR unter

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

C. Personalien

Personelle Änderungen hat es nicht gegeben. Der Verfasser dieses Berichts ist seit dem 25. Mai 2018 Rundfunkdatenschutzbeauftragter des NDR. Seit dem 1. Oktober 2018 unterstützt Frau Ramand den Rundfunkdatenschutzbeauftragten. Auf Vorschlag des NDR Verwaltungsrates erfolgte im Dezember 2021 eine **Wiederernennung** des Rundfunkdatenschutzbeauftragten durch den NDR Rundfunkrat für die Zeit ab dem 25. Mai 2022 für weitere vier Jahre. Für das damit von den Mitgliedern des NDR Verwaltungsrats und den Mitgliedern des NDR Rundfunkrats ausgesprochene Vertrauen sei auch an dieser Stelle gedankt.

Mit Ablauf des Jahres 2021 endete auch der **Vorsitz des Arbeitskreises der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio** (AKDSB), der ohnehin um ein Jahr über die Regeldauer von zwei Jahren hinaus verlängert worden war. Der Vorsitz in diesem Arbeitskreis wird nun vom Datenschutzbeauftragten des Bayerischen Rundfunks übernommen.

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 besteht weiterhin für den Fall der Verhinderung der Rundfunkbeauftragten für den Datenschutz des MDR über einen Zeitraum von länger als 2 Monaten. Vertretungsbedarf gab es im Berichtsjahr allerdings nicht.

D. Wesentliche (rechtliche) Entwicklungen im Berichtszeitraum

Im **Jahr 1996** erschien im Suhrkamp-Verlag eine Untersuchung über die kommerzielle Fernsehwerbung in der BRD in den Jahren von 1956 bis 1989 (Schmidt/Spieß, die Kommerzialisierung der Kommunikation, Frankfurt 1996). Ergebnis: „Die Entwicklung der Medien und der Kommunikation seit dem Zweiten Weltkrieg hat im Rahmen der gesamtgesellschaftlichen Entwicklung in der Bundesrepublik Deutschland zu einer Kommerzialisierung der medienvermittelten Kommunikation geführt, an der Werbung in erheblichem Maße beteiligt gewesen ist“ (S. 32). Anders formuliert: **Formen und Inhalte medienvermittelter Kommunikation folgen primär ökonomischen Interessen**.

25 Jahre später entscheidet das Bundesverfassungsgericht in seinem Beschluss zur Rundfunkfinanzierung (erneut), dass der Gesetzgeber mit der Schaffung der dualen Rundfunkordnung ein Mediensystem geschaffen hat, das den **Risiken einer kommerzialisierten Kommunikation Rechnung** trägt (BVerfG, Beschluss vom 20. Juli 2021 - 1 BvR 2756/20; Hervorhebungen vom Verfasser dieses Berichts):

„Dem öffentlich-rechtlichen Rundfunk kommt im Rahmen der dualen Rundfunkordnung, das heißt im Nebeneinander von öffentlich-rechtlichem und privatwirtschaftlichem Rundfunk, die Erfüllung des klassischen Funktionsauftrags der Rundfunkberichterstattung zu. Er hat die Aufgabe, als Gegengewicht zu den privaten Rundfunkanbietern ein Leistungsangebot hervorzubringen, das einer **anderen Entscheidungsrationalität als der der ökonomischen Anreize** folgt und damit eigene Möglichkeiten der Programmgestaltung eröffnet. Er

hat so zu inhaltlicher Vielfalt beizutragen, wie sie allein über den freien Markt nicht gewährleistet werden kann“ (Rn. 78).

Weiter heißt es in der Entscheidung:

„Die Digitalisierung der Medien und insbesondere die Netz- und Plattformökonomie des Internet einschließlich der sozialen Netzwerke begünstigen […] Konzentrations- und Monopolisierungstendenzen bei Anbietern, Verbreitern und Vermittlern von Inhalten. Sind Angebote zum größten Teil werbefinanziert, fördern sie den publizistischen Wettbewerb nicht unbedingt; auch im Internet können die für die Werbewirtschaft interessanten größeren Reichweiten nur mit den massenattraktiven Programmen erreicht werden. **Hinzu kommt die Gefahr, dass – auch mit Hilfe von Algorithmen – Inhalte gezielt auf Interessen und Neigungen der Nutzerinnen und Nutzer zugeschnitten werden, was wiederum zur Verstärkung gleichgerichteter Meinungen führt. Solche Angebote sind nicht auf Meinungsvielfalt gerichtet, sondern werden durch einseitige Interessen oder die wirtschaftliche Rationalität eines Geschäftsmodells bestimmt, nämlich die Verweildauer der Nutzer auf den Seiten möglichst zu maximieren und dadurch den Werbewert der Plattform für die Kunden zu erhöhen**. Insoweit sind auch Ergebnisse in Suchmaschinen vorgefiltert und teils werbefinanziert, teils von „Klickzahlen“ abhängig. Zudem treten verstärkt nicht-publizistische Anbieter ohne journalistische Zwischenaufbereitung auf.

Dies alles führt dazu, dass es schwieriger wird, zwischen Fakten und Meinung, Inhalt und Werbung zu unterscheiden, sowie zu neuen Unsicherheiten hinsichtlich der Glaubwürdigkeit von Quellen und Wertungen. **Der einzelne Nutzer muss die Verarbeitung und die massenmediale Bewertung übernehmen, die herkömmlich durch den Filter professioneller Selektionen und durch verantwortliches journalistisches Handeln erfolgt**. Angesichts dieser Entwicklung wächst die Bedeutung der dem beitragsfinanzierten öffentlich-rechtlichen Rundfunk obliegenden Aufgabe, durch authentische, sorgfältig recherchierte Informationen, die Fakten und Meinungen auseinanderhalten, die Wirklichkeit nicht verzerrt darzustellen und das Sensationelle nicht in den Vordergrund zu rücken, vielmehr ein vielfaltsicherndes und Orientierungshilfe bietendes Gegengewicht zu bilden (BVerfGE 149, 222 <262 Rn. 80>). Dies gilt gerade in Zeiten vermehrten komplexen Informationsaufkommens einerseits und von einseitigen Darstellungen, Filterblasen, Fake News, Deep Fakes andererseits“ (Rn. 80 f.).“

Im Rahmen einer Entscheidung über die Finanzierung des öffentlich-rechtlichen Rundfunks geht das Gericht nachvollziehbar nicht auf datenschutzrechtliche Belange ein. Die Gefahren kommerzialisierter und digitalisierter Kommunikation lassen sich gleichwohl der Entscheidung entnehmen: Die wirtschaftliche Rationalität der Geschäftsmodelle erfordert nicht nur die möglichst lange Aufmerksamkeit für angepriesene Produkte und Dienstleistungen, sondern möglichst auch umfassende Kenntnisse über die Nutzer*innen bzw. über ihre Daten, um konfektionierte Werbungen zu unterbreiten.

Wozu dies führen kann, hat die **Künstlergruppe Laokoon** eindrucksvoll untersucht. Nach der Maßgabe „Du gibst uns deine Daten und wir sagen dir, wer du wirklich bist." wurden nach der in der EU geltenden Rechtslage anhand von Datensätzen von Facebook und Google (Suchanfragen vergangener Jahre, Metadaten) Wünsche, Persönlichkeitsmerkmale, Ängste erfasst und digitale Doppelgänger geschaffen (www.madetomeasure.online/). Ergebnis: Die digitale Identität ist nicht mehr zu kontrollieren, weil der Handel mit Daten, das Erstellen von Profilen und das sogenannte Microtargetting die Deutungsmacht übernommen haben. Die betroffene Person muss ihr virtuelles Spiegelbild als objektive Realität hinnehmen.

Wie aktuell der Schutz der informationellen Selbstbestimmung ist, zeigt auch die künstlerische Befassung mit dieser Thematik an der **Hochschule für bildende Künste** (HFBK) in Hamburg. Die Hochschule hatte Stipendien für das „Nichtstun" ausgelobt. Eine Gewinnerin war angetreten mit dem Ziel: „Ich will für zwei Wochen keine verwertbaren, personenbezogenen Daten über mich generieren." Die Hochschule begründete das Stipendiat wie folgt: „Das bedeutet umfangreiche Einschränkungen für die 26-jährige Konzepterin und Studentin aus Köln: Kein Smartphone nutzen, keine E-Mails abrufen, nicht online shoppen – allesamt Tätigkeiten, auf die auch viele andere Bewerber*innen verzichten möchten, weil sie zu viel Energie verbrauchen, soziale Beziehungen belasten, zum Konsum verleiten und unkontrollierbare Datenspuren von sich und anderen hinterlassen. Bemerkenswert fand die Jury Mia Hofners Klarheit, mit der sie die Folgen ihres täglichen Handelns reflektiert und sich gleichzeitig bewusst ist, dass sie dem digitalen Datentransfer nicht für immer entkommen kann" (www.hfbk-hamburg.de/de/service/pressemitteilungen/Stipendien-fuer-nichtstun-vergeben/).

Welchen Zweck verfolgt Datenschutz noch einmal?

Das Recht auf informationelle Selbstbestimmung ist „primär als Gewährleistung zu verstehen, die - neben der ungewollten Preisgabe von Daten auch im Rahmen privater Rechtsbeziehungen – insbesondere vor deren intransparenter Verarbeitung und Nutzung durch Private schützt. Es bietet Schutz davor, dass Dritte sich individueller Daten bemächtigen, und sie in nicht nachvollziehbarer Weise als Instrument nutzen, um die Betroffenen auf Eigenschaften, Typen oder Profile festzulegen, auf die sie keinen Einfluss haben und die dabei aber für die freie Entfaltung der Persönlichkeit sowie eine gleichberechtigte Teilhabe in der Gesellschaft von erheblicher Bedeutung sind“ (BGH, Urteil vom 07.07.2020 - VI ZR 250/19, Rn. 57).

Das Dokumentationsprojekt „Made to Measure” und das Stipendium „für das Nichtstun“ machen es deutlich: Wenn man nicht nichts tun möchte, um sich zu schützen, bleibt viel zu tun, um das Recht auf informationelle Selbstbestimmung umfassend zu gewähren, und zwar für alle

- Personen, um sich eine Datenschutzkompetenz anzueignen,
- Verantwortlichen, um gewissenhaft mit personenbezogenen Daten umzugehen,
- Aufsichtsbehörden, um die Rechte und Freiheiten zu überwachen und durchzusetzen.

Für den Gesetzgeber gilt dies ebenfalls. Denn „Metadaten“, also strukturierte Daten, die Merkmale und Eigenschaften anderer Daten beinhalten („Daten über Daten“), können auch ohne spezifische Inhalte – von der betroffenen Person ungewollt und nicht bekannt – eine Biographie entstehen lassen und Auskunft über Gewohnheiten, Vorlieben, Gesundheit usw. geben. Hier gibt es Regelungsbedarf.

Wie sich der Datenschutz in den kommenden Jahren entwickeln wird, bleibt abzuwarten. Der „Koalitionsvertrag 2021–2025 zwischen der SPD, BÜNDNIS 90/DIE GRÜNEN und FDP“ führt dazu aus (Ziffern 467 ff.): „Die Datenschutzgrundverordnung (DSGVO) ist eine gute internationale Standardsetzung. Zur besseren Durchsetzung und Kohärenz des Datenschutzes verstärken wir die europäische Zusammenarbeit, institutionalisieren die Datenschutzkonferenz im Bundesdatenschutzgesetz (BDSG) und wollen ihr rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen. […] Wir schaffen Regelun-

gen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen. Wir setzen uns für eine schnelle Verabschiedung einer ambitionierten E-Privacy-Verordnung ein."

I. Gesetzgebung

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

1. NDR Staatsvertrag

Wie erwähnt, haben die vier Staatsvertragsländer des NDR zum 1. September 2021 einen novellierten NDR Staatsvertrag in Kraft gesetzt. Die bisherigen Vorschriften des NDR Datenschutz Staatsvertrages wurden in den Staatsvertrag ohne Änderungen integriert.

Eingeführt wurde mit dem neuen Staatsvertrag der Zugang zu Informationen für natürliche und (inländische) juristische Personen. Gemäß § 47 Abs. 1 NDR Staatsvertrag gilt nun:

„Jede natürliche oder juristische Person mit Sitz in Deutschland hat nach Maßgabe dieser Bestimmung einen Anspruch auf freien Zugang zu den Informationen, über die der NDR als informationspflichtige Stelle verfügt. Von diesem Anspruch sind Informationen, über die der NDR zu journalistisch-redaktionellen Zwecken verfügt, ausgeschlossen."

Am Ende der Vorschrift ist ein Anrufungsrecht geregelt (§ 47 Abs. 11 NDR Staatsvertrag):

„Antragstellende, die der Ansicht sind, dass der Informationsanspruch zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass nur eine unzulängliche Antwort gegeben worden ist, können den Rundfunkdatenschutzbeauftragten oder die Rundfunkdatenschutzbeauftragte des NDR anrufen."

Der Gesetzgeber hat sich damit der auch vom Verfasser dieses Berichts vertretenen und im Anhörungsverfahren übermittelten Auffassung angeschlossen, dass die Zuständigkeit für die Überprüfung derartiger Anträge nicht der Zuständigkeit der Beauftragten für den Datenschutz und der Informationsfreiheit der Länder unterliegt.

2. Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)

Das TTDSG trat zum 1. Dezember 2021 in Kraft. Dieses Gesetz beinhaltet Vorschriften zum Schutz des Fernmeldegeheimnisses, des Datenschutzes und bislang im Telemediengesetz enthaltene Regelungen. Zugleich hat der Gesetzgeber das Ziel verfolgt, Vorgaben aus der DSGVO und der ePrivacy-Richtlinie auszuformen bzw. umzusetzen.

Insbesondere wird mit dem Gesetz beabsichtigt, das Speichern von und den Zugriff auf Informationen in der Endeinrichtung der nutzenden Personen (Computer, mobile Endgeräte) von einer Einwilligung abhängig zu machen. Regelungsgegenstand ist mithin insbesondere das Verwenden von Cookies und sog. „Identifyern".

3. Gesetz zur Förderung der Betriebsratswahlen und der Betriebsratsarbeit in einer digitalen Arbeitswelt (Betriebsrätemodernisierungsgesetz)

Am 18. Juni 2021 ist das Betriebsrätemodernisierungsgesetz in Kraft getreten. Ziele des Gesetzes sind u. a. die Wahlen von Betriebsräten zu vereinfachen und die Rechte des Betriebsrats bei der Weiterbildung, dem Einsatz von künstlicher Intelligenz und bei mobiler Arbeit zu stärken. Mit dem Gesetz wird nun auch klarstellend geregelt, dass Personalvertretungen nicht eigene Verantwortliche im Sinne der DSGVO sind, sondern als Teil eines Unternehmens angesehen werden. Ein Unternehmen bleibt mithin allein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

§ 79a Betriebsverfassungsgesetz lautet:
„Datenschutz
Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtli-

chen Vorschriften. Arbeitgeber und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. § 6 Absatz 5 Satz 2, § 38 Absatz 2 des Bundesdatenschutzgesetzes gelten auch im Hinblick auf das Verhältnis der oder des Datenschutzbeauftragten zum Arbeitgeber."

Die entsprechende Regelung findet sich auch in § 69 Bundespersonalvertretungsgesetz. Personalvertretungen werden mithin als organisationsinterne Einrichtungen qualifiziert, nicht aber nach außen rechtlich verselbstständigte Institutionen. Datenschutzrechtlich verantwortlich bleibt mithin die Dienststelle (also das Unternehmen (der NDR)). Die gesetzgeberische Klarstellung ist zu begrüßen, weil die Frage, ob Personalvertretungen eigene Verantwortliche sind oder nicht, lange Zeit umstritten war. Eindeutig bestätigt ist damit auch die **Zuständigkeit des Rundfunkdatenschutzbeauftragten für die Personalvertretungen des NDR**, weil sich die Aufsicht über die gesamte Tätigkeit des NDR erstreckt (§ 46 Abs. 1 S. 1 NDR Staatsvertrag).

4. Entwicklungen auf Europäischer Ebene

Im Blick gehalten werden müssen insbesondere die Aktivitäten des EDSA und der EU-Kommission.

Der **Europäische Datenschutzausschuss** (EDSA) stellt eine unabhängige europäische Einrichtung dar. Ziel ist die einheitliche Anwendung der Datenschutzvorschriften in der Europäischen Union und die Förderung der Zusammenarbeit zwischen allen Datenschutzbehörden der EU.

Der aus Vertreter*innen der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten zusammengesetzte Ausschuss gibt Anleitungen und Leitlinien heraus, etwa hinsichtlich der Übermittlung personenbezogener Daten von Behörden oder öffentlichen Stellen an öffentliche Stellen in Drittländern oder internationale Organisationen, soweit solche Übermittlungen nicht durch einen von der Europäischen Kommission angenommenen Angemessenheitsbeschluss abgedeckt sind.

Dies ist beispielsweise von Bedeutung für Datenübermittlungen in die USA nach Wegfall des Privacy Shields aufgrund der einschlägigen Rechtsprechung des EUGH.

Auch die Tätigkeiten der **EU-Kommission** entfalten Auswirkungen für den NDR und alle Beteiligungsunternehmen: So hat die Kommission am 04. Juni 2021 zwei Beschlüsse zu sogenannten Standardvertragsklauseln erlassen: Mit dem

- **DURCHFÜHRUNGSBESCHLUSS (EU) 2021/915 DER KOMMISSION** vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates

  und dem
- **DURCHFÜHRUNGSBESCHLUSS (EU) 2021/914 DER KOMMISSION** vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates

hat die EU-Kommission von ihrem Recht Gebrauch gemacht, Standardvertragsklauseln zur Auftragsverarbeitung gemäß Art. 28 Abs. 7 DSGVO zu verabschieden. Der zuletzt genannte Beschluss betrifft Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer und ist damit eine Folge des Urteils des EuGH zum Wegfall des Privacy Shields. Die neuen Standardvertragsklauseln beinhalten geeignete Garantien gemäß Art. 46 Abs. 2 c) DSGVO, die dann zur Anwendung kommen können, wenn – wie derzeit – kein Angemessenheitsbeschluss der EU-Kommission in Bezug auf die Datenverarbeitung im Drittland vorliegt.

Zumindest datenschutzrechtlich wurden auch die Folgen des **Brexit** geglättet: Der Austritt Großbritanniens aus der EU zum 31.01.2020 hatte zur Folge, dass Großbritannien zu einem Drittland im datenschutzrechtlichen Sinne geworden war. Im Brexit-Deal wurde zunächst nur eine Übergangsvorschrift für Übermittlungen von personenbezogenen Daten aus der EU in das Vereinigte Königreich Großbritannien und Nordirland festgeschrieben.

Der **DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION vom 28.6.2021** gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich hat nun festgestellt:

„Für die Zwecke des Artikels 45 der Verordnung (EU) 2016/679 gewährleistet das Vereinigte Königreich ein angemessenes Schutzniveau für personenbezogene Daten, die im Rahmen der Verordnung (EU) 2016/679 aus der Europäischen Union an das Vereinigte Königreich übermittelt werden."

Mit anderen Worten: Die Übermittlung personenbezogener Daten in das Vereinigte Königreich bleibt derzeit weiterhin grundsätzlich möglich. Allerdings bestehen begründete Zweifel, ob dies so bleibt: Denn die britische Regierung plant eine Reform des Datenschutzes mit dem Ziel einer „wachstums- und innovationsfreundlichen" Regulierung. Ob diese dem Niveau der DSGVO entsprechen wird, darf bezweifelt werden, weil Datenschutz als Hemmnis bei internationalen Datenübertragungen gesehen wird. Ein Sprecher der EU-Kommission reagierte bereits mit dem Hinweis, dass der aktuelle Durchführungsbeschluss jederzeit widerrufen werden könnte.

Am 28. Januar 2021 wurde der **Europäische Datenschutztag** begangen. Bei der (Online-) Veranstaltung des Bundesministerium des Innern, für Bau und Heimat wurde die **Datenschutzkonvention 108 des Europarats** gewürdigt, die bereits ihren 40. Geburtstag hatte. Die Datenschutzkonvention 108 war der erste völkerrechtlich verbindliche Vertrag zum Datenschutz und Vorbild für weitere datenschutzrechtliche Regelungen.

Das **Europäische Parlament** hat sich am 25. März 2021 mit der Evaluierung der DSGVO (Entschließung des Europäischen Parlaments vom 25. März 2021 zu dem Bewertungsbericht der Kommission über die Durchführung der Datenschutzgrundverordnung zwei Jahre nach Beginn ihrer Anwendung (2020/2717(RSP)) befasst und neben diversen Forderungen insgesamt begrüßt,

- „dass die DSGVO zu einer weltweiten Norm für den Schutz personenbezogener Daten geworden ist und bei der Ausarbeitung von Normen eine gewisse Konvergenz bewirkt;

– dass die EU durch die DSGVO eine Vorreiterrolle in der internationalen Debatte über Datenschutz eingenommen hat und zahlreiche Drittländer ihre Datenschutzgesetze an die Bestimmungen der DSGVO angeglichen haben."

5. Bußgelder

Nach Art. 58 Abs. 2 lit. i) in Verbindung mit Art. 83 DSGVO können datenschutzrechtliche Aufsichtsbehörden Bußgelder gegen Unternehmen verhängen, wenn gegen datenschutzrechtliche Vorschriften verstoßen wurde.

Die für WhatsApp zuständige irische Datenschutzbehörde DPC hat Anfang September 2021 ein solches Bußgeld gegen die Facebook-Tochter WhatsApp in Höhe von 225 Millionen Euro verhängt, weil der Messengerdienst nicht hinreichend transparent über die Verwendung der Daten der Nutzer*innen informiere. Es sei unklar, welche Daten verarbeitet und an den Mutterkonzern übermittelt werden. Ob der Bußgeldbescheid in Rechtskraft erwächst, ist noch nicht klar. WhatsApp bezeichnete die Maßnahme „vollkommen unangemessen" und hat rechtliche Schritte angekündigt.

Auch andere Aufsichtsbehörden haben gegen große Konzerne Bußgelder verhängt: Die französische Datenschutzbehörde CNIL hatte Ende des Jahres 2020 Google und Google Irland eine Geldbuße von 100 Millionen Euro auferlegt, Amazon hat einen Bescheid über 746 Millionen Euro erhalten. Die Datenschutzgrundverordnung sieht vor, dass derartige Bußgelder von bis zu vier Prozent des Jahresumsatzes möglich sind. Insgesamt ist festzuhalten, dass die Aufsichtsbehörden zunehmend mehr Bußgelder verhängen. Allein im dritten Quartal 2021 belief sich die Summe der verhängten Bußgelder in der EU auf 984,47 Millionen Euro (wobei noch nicht alle Bescheide rechtskräftig wurden).

II. Rechtsprechung

Die Tragweite gerichtlicher Entscheidungen mit datenschutzrechtlichem Bezug erweitert sich kontinuierlich. Der folgende Überblick beinhaltet nur einen Auszug wichtiger Entscheidungen aus dem Berichtsjahr.

1. Zuständigkeiten und Klagebefugnisse von Aufsichtsbehörden

Mitte des Jahres 2021 hat der EuGH (Rechtssache C-645-19, Urteil vom 15.06.2021) ein Urteil zur internationalen Zuständigkeit und zu Kompetenzen von Aufsichtsbehörden untereinander gefällt.

Das in der DSGVO verankerte „One-Stop-Shop"-Verfahren soll für Verantwortliche und Betroffene eine zentrale datenschutzrechtliche Anlaufstelle schaffen. Der EuGH hat sich im Einzelnen mit Zuständigkeitsfragen befasst und festgehalten, dass die federführende Datenschutzbehörde zuständig ist, einen Beschluss zu erlassen, mit dem festgestellt wird, dass eine grenzüberschreitende Verarbeitung gegen die Vorschriften der DSGVO verstößt. Allerdings bleiben in Ausnahmefällen auch andere nationale Aufsichtsbehörden unter bestimmten Voraussetzungen zuständig. Insgesamt hat das Gericht aber die **Aufsichtsbehörden gestärkt**, indem es entschied, dass eine Klage einer Aufsichtsbehörde auch dann möglich sei, wenn das nationale Recht eine solche Klagebefugnis nicht explizit geregelt habe. Die Befugnisse dazu ergäben sich bereits unmittelbar aus der DSGVO selbst.

2. Bundesverfassungsgericht: Geldentschädigungen für Datenschutzverstöße

In einem Fall **unerwünschte Werbe-E-Mails** betreffend, hat das Bundesverfassungsgericht sich mit der Frage der Voraussetzungen für einen Geldentschädigungsanspruch nach Art. 82 DSGVO befasst.

Das Amtsgericht Goslar hatte keinen Schaden erkannt und die Klage auf Geldentschädigung wegen Persönlichkeitsrechtsverletzung insoweit abgewiesen: Da es sich lediglich um eine nicht erwünschte Werbe-E-Mail gehandelt habe, die „nicht zur Unzeit versandt worden" und deutlich als Werbung zu erkennen gewesen sei, könne nicht davon ausgegangen werden, dass ein Anspruch auf Schadensersatz entstanden sei.

Das Bundesverfassungsgericht hat dazu festgestellt (BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 14. Januar 2021 - 1 BvR 2853/19 -), dass das Amtsgericht Art. 101 Abs. 1 Satz 2 GG verletzt habe (Entzug des gesetzlichen Richters). Denn es

hätte zunächst den Gerichtshof der Europäischen Union mit der Sache befassen müssen. Grund:

„Dieser Geldentschädigungsanspruch ist in der Rechtsprechung des Gerichtshofs der Europäischen Union weder erschöpfend geklärt noch kann er in seinen einzelnen, für die Beurteilung des im Ausgangsverfahren vorgetragenen Sachverhalts notwendigen Voraussetzungen unmittelbar aus der DSGVO bestimmt werden."

Die dadurch angegangene grundsätzliche Klärung, unter welchen Voraussetzungen Schadensersatz zu leisten ist, ist zu begrüßen, um Bagatell- bzw. Erheblichkeitsgrenzen rechtssicher zu definieren.

Der **BGH** hatte in einem anderen Fall keinen Schadensersatz für eine **journalistische Datenverarbeitung** erkannt: In der kurzen Entscheidung hat das Gericht (Beschluss vom 16.02.2021 - VI ZA 6/20) festgestellt, dass ein Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO im zu beurteilenden Fall nicht bestehen könne, „weil aufgrund der Öffnungsklausel des Art. 85 DSGVO Datenverarbeitungen zu journalistischen Zwecken von den die Rechtmäßigkeit der Datenverarbeitung betreffenden Vorschriften in Art. 6 und Art. 7 DSGVO durch nationale Regelungen ausgenommen worden sind."

Gemeint ist damit Folgendes:

Der BGH geht von der **fortgeltenden Anwendbarkeit des Kunsturhebergesetzes** (KUG) aus. Danach wird die Zulässigkeit von Bildveröffentlichungen von Personen nach einem abgestuften Schutzkonzept (namentlich der §§ 22, 23 KUG) beurteilt.

Nach diesem Konzept dürfen Bildnisse einer Person nur mit deren Einwilligung veröffentlicht werden. Liegt eine solche Einwilligung nicht vor, muss das Bild dem Bereich der Zeitgeschichte oder einem der anderen Ausnahmetatbestände zugeordnet werden können. Diese hier sehr grob dargestellten Grundsätze gelten auch unter den Bedingungen der DSGVO fort:

„Der Anwendbarkeit der §§ 22, 23 KUG steht im hier betroffenen journalistischen Bereich die zwischenzeitlich eingetretene Geltung der Verordnung (EU) 2016/679 des

Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [DSGVO] schon deshalb nicht entgegen, weil aufgrund der Öffnungsklausel des Art. 85 DSGVO Datenverarbeitungen zu journalistischen Zwecken durch die Anbieter von Telemedien von den die Rechtmäßigkeit der Datenverarbeitung betreffenden Vorschriften in Art. 6 und Art. 7 DSGVO durch nationale Regelungen ausgenommen worden sind (§ 1 Abs. 1 Hs. 2, § 57 Abs. 1 Satz 4 des Staatsvertrags für Rundfunk und Telemedien [Rundfunkstaatsvertrag - RStV] in der seit dem 25. Mai 2018 geltenden Fassung) und die §§ 22, 23 KUG im Hinblick auf die Beurteilung der Zulässigkeit von Bildveröffentlichungen im journalistischen Bereich als die Öffnungsklausel des Art. 85 DSGVO ausfüllende Gesetze anzusehen sind [...]."

Was das im Einzelnen für die Praxis bedeutet, wird unter E. II. 2 c) dargestellt.

3. Arbeitsrecht: Permanentes und uneingeschränktes Einsichtsrecht in elektronisch geführte Personalakten für Betriebsratsvorsitzende unzulässig

Das LAG Düsseldorf hatte sich zu befassen mit einer Regelung eines Betriebes, nach der die Betriebsratsvorsitzenden einzelner Betriebe in einer Gesamtbetriebsvereinbarung dauerhafte und unbeschränkte Einsichtsrechte in die elektronisch geführten Personalakten hatten.

Mit Beschluss vom 23.06.2020 (Az. 3 TaBV 65/19) kassierte das Gericht diese Regelung. Diese sah u. a. vor:

„Der Gesamtbetriebsratsvorsitzende und der örtliche Betriebsratsvorsitzende erhält permanenten Zugriff auf die elektronische Personalakte mit Ausnahme der Akten der Leitenden Mitarbeiter und der Mitarbeiter des Personalbereiches. Die örtlichen Betriebsratsvorsitzenden erhalten dabei Zugriff auf die Akten des Wahlbetriebes, für den sie zuständig sind. Der Gesamtbetriebsratsvorsitzende erhält Zugriff auf die Akten des gesamten Unternehmens."

Das Gericht hat dazu festgestellt:

„In der von der individuellen Zustimmung der Arbeitnehmer unabhängigen, kollektivrechtlichen Regelung eines permanenten lesenden Zugriffsrechts der Betriebsratsvorsitzenden bzgl. der elektronischen Personalakten der Arbeitnehmer ihres Wahlbetriebes liegt ein Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts der betreffenden Arbeitnehmer. Denn damit werden einem Dritten, nämlich den jeweiligen Betriebsratsvorsitzenden, persönliche Lebenssachverhalte wie die Stammdaten der betreffenden Arbeitnehmer, bestehende Unterhaltspflichten, Pfändungen, vertragliche Absprachen mit der Beteiligten zu 2.), erhaltene Abmahnungen und vieles anderes mehr, eben der gesamte Inhalt ihrer elektronisch geführten Personalakte, offenbart, ohne dass dies von ihrer vorherigen Zustimmung abhängig wäre oder sie auch nur davon erführen. Noch dazu ist das Leserecht der Betriebsratsvorsitzenden nach dem klaren Wortlaut der Ziffer 8.3 GBV EFM ein permanentes, also zeitlich in keiner Weise eingeschränktes. Jederzeit kann ein Betriebsratsvorsitzender danach auf den gesamten Personalakteninhalt Zugriff nehmen."

Datenschutzrechtlich waren die auch im Beschäftigtendatenschutz zu beachtenden Grundsätze der Zweckbindung und Datenminimierung überschritten worden, weshalb auch im Wege der Auslegung der Vorschrift kein eingeschränkter Anwendungsbereich verblieb.

4. BGH: Reichweite eines datenschutzrechtlichen Auskunftsersuchens

Immer wieder beschäftigt die Gerichte die Frage, in welcher Inhaltstiefe Auskünfte über verarbeitete Daten zu erteilen sind. Der BGH (Urteil vom 15.06.2021 - VI ZR 576/19) hatte nun Gelegenheit, diese Sache zu entscheiden:

- Der Anspruch auf Auskunft folgt unmittelbar aus Art. 15 DSGVO.
- Nach Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.

- Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, sieht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist.
- Wenn sich der Auskunftspflichtige (das Unternehmen) hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet, kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen.
- Wird ein Auskunftsbegehren angesichts bereits erteilter Auskünfte unter anderem dahingehend präzisiert, dass weitergehende Auskünfte hinsichtlich der gesamten noch nicht mitgeteilten Korrespondenz der Parteien, einschließlich etwaiger Telefon-, Gesprächs- und Bewertungsvermerke, geltend gemacht werden, muss die Vollständigkeit geprüft werden.
- Auskunftsgegenstände nach Art. 15 Abs. 1 DSGVO sind gemäß Art. 4 Nr. 1 Halbsatz 1 DSGVO personenbezogene Daten. Dies sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- Nach der Rechtsprechung des BGH beschränken diese sich nicht auf sensible oder private Informationen, sondern umfassen „potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist“.
- Schreiben einer Person an ein Unternehmen sind grundsätzlich ihrem gesamten Inhalt nach als personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO anzusehen. Die personenbezogene Information besteht bereits darin, dass sich der Kläger dem Schreiben gemäß geäußert hat. Dass die Schreiben

dem Kläger bereits bekannt sind, schließt für sich genommen entgegen der Auffassung des Berufungsgerichts den datenschutzrechtlichen Auskunftsanspruch nicht aus. Die Auskunft soll diesbezüglich aber Aufschluss darüber geben, ob die im Schriftverkehr enthaltenen personenbezogenen Daten aktuell verarbeitet, insbesondere gespeichert werden.

- Eine Feststellung in einer Auskunft, dass eine Korrespondenz keine Daten über die bereits erteilten Auskünfte hinaus enthält, ist zulässig. Mit einer solchen Negativauskunft ist der Auskunftsanspruch hinsichtlich dieses Auskunftsgegenstandes erfüllt.

E. Tätigkeiten des Rundfunkdatenschutzbeauftragten im Jahr 2021

Der Austausch und die Zusammenarbeit mit anderen Datenschutzbeauftragten und Aufsichtsbehörden ist nicht nur rechtlich vorgeschrieben, sondern für die Fülle der zu erledigenden Aufgaben unabdingbar. Im Folgenden wird zunächst eingegangen auf die Zusammenarbeit mit den datenschutzrechtlichen Aufsichtsbehörden im öffentlich-rechtlichen Rundfunk, mit den Datenschutzbehörden der Länder und des Bundes und dem Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio.

I. Organisationsstrukturen/Zusammenarbeit mit anderen Aufsichtsbehörden

Grundsätzlich können drei Gruppen unterschieden werden, in denen ein Wissenstransfer und gegenseitige Hilfen vorgenommen werden:

- Die **Rundfunkdatenschutzkonferenz** (RDSK): Das sind die als Aufsichtsbehörden tätigen Personen im öffentlich-rechtlichen Rundfunk.
- Der **Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio** (AKDSB): Das Forum aller Datenschutzbeauftragten von ARD, ZDF, Deutschlandradio, dem ORF und ARTE.
- Die **Datenschutzkonferenz** (DSK): Das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder.

1. Die Rundfunkdatenschutzkonferenz (RDSK)

Der Vorsitz der RDSK wurde zu Beginn des Jahres 2021 vom Verfasser dieses Berichts vom Rundfunkdatenschutzbeauftragten des Bayerischen Rundfunks, des Saarländischen Rundfunks, des Westdeutschen Rundfunks, des Deutschlandradios und des Zweiten Deutschen Fernsehens übernommen. Stellvertretende Vorsitzende ist die Datenschutzbeauftragte des Rundfunk Berlin-Brandenburg. Weitere Mitglieder sind

- 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

In einer **Geschäftsordnung**, einer „**Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten**“ und einer „**Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten**“ sind die Verfahrensweise und die Zuständigkeiten der RDSK niedergelegt. Alle Dokumente und weitere Informationen können seit Beginn des Jahres 2021 auf der Homepage der RDSK abgerufen werden:

www.rundfunkdatenschutzkonferenz.de/

Weiterhin wurde unter den Mitgliedern vereinbart, dass im Blick zu haltende Themen nach einem Federführungsprinzip aufgeteilt werden, um die Vielzahl der relevanten rechtlichen Entwicklungen im Griff zu behalten.

b) Tätigkeitsschwerpunkte der RDSK

Kerngeschäft sind die **Öffentlichkeitsarbeit und inhaltliche Positionierungen** durch Empfehlungen, Stellungnahmen und Orientierungshilfen. Der Bedarf an öffentlichen Positionierungen ist größer, als die Anzahl der bislang erschienenen Veröffentlichungen es vermuten lässt. Allein die engen Personalkapazitäten lassen derzeit nicht mehr zu. Die Veröffentlichungen sind zu finden unter

www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen.

Hinzugekommen waren zuletzt eine Entschließung zu der Clubhouse-App, einer Applikation für Audio-Talkshows, mit der sich die Nutzenden Gespräche anhören und an Diskussionen teilnehmen können. Die RDSK hatte sich im Februar 2021 dazu geäußert und datenschutzrechtliche Bedenken erläutert. Zudem wurde ein Positionspapier mit dem Titel „Datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen“ veröffentlicht“, um die grundlegenden Anforderungen an derartige Systeme, die vermehrt zum Einsatz kommen, festzulegen.

Weitere zu behandelnde Themen waren

- das Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder nach § 18 Abs. 1 S. 4 BDSG,
- die Nutzung von Drittplattformen durch die Rundfunkanstalten,
- Aufsichtszuständigkeiten bei Kooperationen im Programmbereich,
- die Anwendung von Art. 83 DSGVO (Bußgeldrahmen),
- die Umsetzung Art. 35 Abs. 4 DSGVO („Blacklist“ für eine Datenschutzfolgeabschätzung)
- die Auswirkungen des TTDSG auf die Telemedienangebote der Rundfunkanstalten,
- der Einsatz der Luca-App.

Zudem hat die RDSK im Rahmen einer Abfrage der EU-Kommission zur „Umsetzung der DSGVO auf nationaler Ebene“ (Views of the DPAs on the national im-

plementation of some GDPR and LED provisions) Stellung genommen, um den Evaluierungsprozess zu begleiten.

c) Zusammenarbeit mit der Datenschutzkonferenz

Im Mai und Dezember 2021 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 in der regelmäßig stattfindenden Runde aktuelle Themen besprochen: Auf der Tagesordnung standen aktuelle Entwicklungen im (europäischen) Datenschutz, Berichte über die Tätigkeitsschwerpunkte der Aufsichtsbehörden, die Evaluation des Bundesdatenschutzgesetzes, der Einsatz der Luca-App durch öffentliche Stellen, Kollaborationssysteme und das TTDSG.

Auch die Teilnahme von Mitgliedern der RDSK an den Arbeitskreisen AK Technik, AK Grundsatzfragen und AK Medien der Datenschutzkonferenz ist fester Bestandteil des Wissenstransfers, um der stetig wachsende Befassung mit datenschutzrechtlich relevanten Themen und der steigenden Komplexität der zu beurteilenden Sachverhalte zu begegnen.

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

Die regelmäßig zweimal im Jahr durchgeführten Sitzungen bzw. Videokonferenzen des AKDSB wurden im Jahr 2021 ergänzt durch weitere, halbtägliche Videokonferenzen, die dauerhaft im Abstand von zwei Monaten durchgeführt werden sollen. Die Zunahme an datenschutzrechtlich relevanten Themen, das Erfordernis nach zügigeren Entscheidungen und der erhöhte Abstimmungsbedarf durch gemeinsame Vorhaben der Rundfunkanstalten machen dies erforderlich. Zur Selbstvergewisserung und Strukturierung der Arbeit hat sich der AKDSB zudem eine Geschäftsordnung gegeben.

Als **Vorsitzender des AKDSB** waren die Termine zu organisieren, Tagesordnungen zu erstellen und Sitzungen zu leiten. Inhaltlich ging es um folgende Schwerpunkte:

- Rundfunkteilnehmerdatenschutz

- Umsetzung des 23. Rundfunkänderungsstaatsvertrags beim Beitragsservice
- Errichtung eines Kundenkontaktmanagements beim Beitragsservice
- Elektronische Übermittlung von Daten an Vollstreckungsbehörden
- Elektronische Datenschutzmanagement-Systeme
- Anforderungen an Authentisierungen
- Datenkategorien und Schutzbedarfe: Vereinheitlichung von Standards in den Rundfunkanstalten
- Datensicherheit: Implementierung von Schutzsystemen zur Abwehr feindlicher Angriffe
- Anforderungen und Abgrenzungen von Joint-Controller-Vereinbarungen und Auftragsverarbeitungen/Überarbeitung von Vertragsmustern
- Einsätze von Nutzungsmessungsverfahren in Telemedienangeboten
- Personalisierung von Mediatheken
- Überarbeitung von Social Media Guidelines (datenschutzrechtliche Handlungsanweisungen für Telemedienangebote)
- Kinderdatenschutz in Apps, Anforderungen an Logins
- Onlineschulungen der Medienakademie
- Evaluierung der Datenschutzgesetzgebung, – politik und -rechtsprechung
- Neue Standardvertragsklauseln der EU-Kommission
- Verhaltensregeln für Cloud Anbieter (EU Cloud Code of Conduct)
- Künstliche Intelligenz und Medienprivileg
- Terminbuchungstools
- Harmonisierungsprojekt (D)ein SAP

Die bisherigen zeitlichen Planungen für das zuletzt erwähnte ARD-Strukturprojekt zur EDV-Harmonisierung, namentlich das Projekt der **Harmonisierung und Konsolidierung der Geschäftsprozesse und der dezentralen SAP-Systeme der einzelnen Rundfunkanstalten in eine zentrale SAP-Systemlandschaft**, konnten die beteiligten Rundfunkanstalten aufgrund der Komplexität nicht einhalten. Die datenschutzrechtliche Befassung dauert mithin an. Der AKDSB hat seine datenschutzrechtlichen Empfehlungen abgegeben und sich intensiv mit den einzelnen Teilprojekten

- Finanzen,
- Controlling,

- Beschaffung, Warenwirtschaft, Vertragswesen,
- Cloud-Anwendungen,
- Dienstreisen sowie

unterstützenden Systemen und Anwendungen befasst. Zu bewerten waren dabei Nutzermanagementsysteme, Löschkonzepte, Anforderungen an Datenmigrationen, das Schnittstellenmanagement sowie Dokumenten- und Datenarchive.

In den genannten Social-Media-Guidelines werden für die Praxis relevante Ausführungen gemacht über alle datenschutzrechtliche Belange, die bei Telemedienangeboten zu beachten sind, also bei

- der Verbreitung von Inhalten mittels Apps,
- einer Auftragsvergabe an Dritte,
- Chats, Foren, Gästebücher, Kommentarfunktionen,
- spezifischen Kontaktmöglichkeiten (Mailkontakte, Kontaktformularen, Newslettern),
- dem Einsatz von Cookies und anderen Technologien,
- der Gestaltung von Datenschutzerklärungen,
- der Nutzung von Drittplattformen,
- Embeddings,
- Gewinnspielen,
- Instant Messaging,
- den spezifischen Anforderungen des Minderjährigen-Datenschutzes,
- der Personalisierung von Angeboten (Mediatheken),
- Votings,
- Web-Analysen und
- organisatorischen Fragen.

Die Leitlinien sollen den Verantwortlichen eine Hilfestellung bei der Erstellung und Gestaltung der Telemedienangebote geben und stellen dazu die wesentlichen Anforderungen praxisgerecht und kompakt dar. Die Bearbeitung dauert an.

Eine Schnittmenge der Mitglieder des AKDSB, und zwar die Datenschutzbeauftragten der Kooperationspartner des IVZ (das Informations-Verarbeitungs-Zentrum von

ARD und Deutschlandradio), haben sich zudem über Maßnahmen zur Verbesserung des Austausches zwischen dem IVZ und den Datenschutzbeauftragten der Kooperationspartner des IVZ ausgetauscht und geeinigt. Zudem wurden die anzuwendenden Rechtsgrundlagen für das IVZ erörtert und eine stärkere Einbeziehung des Datenschutzbeauftragten des IVZ verabredet.

Überdies gab es einen Austausch mit zwei **Datenschutzbeauftragten der Schweizerischen Radio- und Fernsehgesellschaft** (SRG SSR) über die Organisation des Datenschutzes im öffentlich-rechtlichen Rundfunk in Deutschland, Österreich und der Schweiz, über die Rolle und Zuständigkeiten von behördlichen Datenschutzbeauftragten und Aufsichtsbehörden, über ausgewählte Schwerpunkte in der jeweiligen aktuellen Praxis sowie über den Schutz sensibler journalistische Daten von Medienunternehmen. **Aufgrund eines entsprechenden Beschlusses des AKDSB wurden die beiden Datenschutzbeauftragten der SRG SSR als Mitglieder in den Arbeitskreis aufgenommen**.

II. Tätigkeitsschwerpunkte bezüglich Datenverarbeitungen im NDR

Datenschutzrechtliche Aufsichtsbehörden haben **präventive und repressive Aufgaben**. Zu den repressiven Aufgaben gehört es zum Beispiel, Datenschutzverstöße von Amts wegen oder aufgrund von Hinweisen und Beschwerden zu ahnden. **Die präventiven Aufgaben sind aber seit Geltung der Datenschutzgrundverordnung rechtlich und tatsächlich angewachsen**: Eine Vielzahl von Befugnissen aus dem Aufgabenkatalog der Aufsichtsbehörden richtet sich auf Aufklärung, Beratung, Information, Bildung und damit darauf, Verstößen vorzubeugen und Entwicklungen, die datenschutzrechtlichen Vorschriften nicht entsprechen würden, zu vermeiden.

Die Effektivität eines modernen Datenschutzrechts und der Erfolg der Kontrollfunktion einer Aufsichtsbehörde basiert daher auf zeitlichen, prozeduralen und organisatorischen Maßgaben. Richtigerweise erfolgt die Einbindung des Rundfunkdatenschutzbeauftragten möglichst

- frühzeitig, d. h. vor Aufnahme einer neuen oder veränderten Datenverarbeitung,
- unter Berücksichtigung von festgelegten Verfahrensabläufen und

– nach Maßgabe von klaren Aufgabenzuschreibungen.

Der Kern der Tätigkeit lag im Berichtsjahr folglich im Bereich der präventiven Aufgaben: Beratungen wurden aus allen Bereichen angefragt, also

– hinsichtlich der Programme und der Programmverbreitung,
– des Rundfunkteilnehmerdatenschutzes,
– des Beschäftigtendatenschutz und bei
– Organisations- und Strukturprojekten der Verwaltung und Produktion.

Die andauernde pandemische Lage hat weiterhin Beratungsbedarf beim Beschäftigtendatenschutz ausgelöst. Auch die Begleitung von **Organisations- und Strukturprojekten** nimmt großen Raum ein, zum einen durch die Einführung neuer Systeme, zum anderen aufgrund der Ablösung bestehender Anwendungen und die Einschaltung Dritter im Wege der Auftragsverarbeitung.

1. Zur Umsetzung der DSGVO

Im Tätigkeitsbericht für das Jahr 2020 wurde dargelegt, dass die von der Datenschutzgrundverordnung geforderten Strukturen, Erklärungen, Informationen, Instrumente und Dokumentationspflichten zwar grundsätzlich umgesetzt sind, es allerdings noch Handlungsbedarf bezüglich des Verfahrensverzeichnisses nach Art. 30 DSGVO gibt. Zum Nachweis der Einhaltung der Datenschutzgrundverordnung soll jedes verantwortliche Unternehmen oder der Auftragsverarbeiter ein Verzeichnis der Datenverarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Das praktische Problem mit dieser Anforderung ist, dass das Verzeichnis zwar einen zusammenfassenden Überblick über die Verarbeitungen gibt und der Verantwortliche sich damit der Verarbeitungen und deren Risiken versichern kann, sich aber der praktische Nutzen kaum entfaltete. Im NDR wurde die Anforderung daher oftmals als bloßer Verwaltungsaufwand ohne Ertrag angesehen. Hinzu kam, dass bereits ähnliche Verzeichnisse existierten, wenn auch nicht mit allen Pflichtangaben aus der DSGVO.

Um in dieser Sache voranzukommen wurde daher ein Vorschlag unterbreitet, wie eine Zusammenführung zweier Verzeichnisse vorgenommen werden kann mit dem Ziel,

- die gesetzliche Anforderung des Führens eines sog. Verfahrensverzeichnisses vollständig erfüllen,
- mit einer Verschlagwortung die Datenbank als Arbeitsmittel nutzbar zu machen, so dass die Beschäftigten für sich relevante und geeignete Anwendungen zur Bewältigung der Arbeit finden können.

Im Übrigen ist festzuhalten, dass noch immer mit Blick auf die DSGVO von einer gelungenen Regulierung ausgegangen werden kann und dass die Umsetzung dieser an die Dynamik der Datenverarbeitungen geknüpft ist: Die Anforderungen sind mithin stets zu überprüfen und auf die neuen oder veränderten Prozesse anzuwenden.

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

Nicht nur im Layout, wie etwa im Falle der Datenschutzerklärung von tagesschau.de (abrufbar unter www.tagesschau.de/datenschutzerklaerung-100.html#Kontaktdaten_des_Verantwortlichen), sondern auch inhaltlich sind immer wieder Änderungen oder Ergänzungen der entsprechenden Erklärungen der vom NDR verantworteten Telemedienangebote (ndr.de, tagesschau.de einschließlich der HbbTV-App der tagesschau, ARD Quiz App sowie weitere Angebote (NDR Text in HbbTV, das NDR Intranet, interne Foren) notwendig. Dies beispielsweise deshalb, weil bestimmte Tools und Services entfallen oder neu aufgenommen werden (etwa Techniken zur Darstellung von Autoplay-Videovorschauen für Livestreams oder einzelne Videos, Messenger-Dienste).

Eine stets aktuelle Datenschutzerklärung eines Telemedienangebots oder einer App ist unerlässlich, um die Datensouveränität der Nutzenden zu wahren und Vertrauen zwischen einer Rundfunkanstalt und dem Publikum zu schaffen. Die Datenschutzerklärungen müssen deshalb vollständig, transparent und verständlich darlegen, welche Daten in welcher Weise verarbeitet werden. Grundpfeiler einer Datenschutzerklärung sind das Gebot der Transparenz und die Pflicht zur umfassenden Information über Datenverarbeitungen bei der Nutzung von Telemedienangeboten: Die Datenschutzerklärung ist der „Beipackzettel" des Onlineangebots.

Die aktuellen Erklärungen sind umfangreich und erfüllen die gesetzlichen Gebote. In manchen Teilen gehen sie möglicherweise über die Anforderungen im Sinne einer möglichst umfassenden Information hinaus. Dies geht auch zurück auf entsprechende Anfragen von Nutzenden und scheint daher als vertrauensbilde Maßnahme hilfreich und nützlich.

b) Internetseite des Rundfunkdatenschutzbeauftragten

Als weiteres Informationsangebot und Instrument der Öffentlichkeitsarbeit steht die Seite des Rundfunkdatenschutzbeauftragten des NDR zur Verfügung (www.ndr.de/der_ndr/unternehmen/organisation/Datenschutz-beimNDR,datenschutz6.html), die alle wesentlichen Rechtsgrundlagen, Berichte und Erläuterungen sowie Informationen in Leichter Sprache dauerhaft bereitstellt. Hier wird auch auf weitere Angebote, etwa dem Datenschutz beim Beitragsservice, die Rundfunkdatenschutzkonferenz und das Virtuelle Datenschutzbüro (ein gemeinsames Angebot von Datenschutzinstitutionen unter der Verantwortung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein) verlinkt.

c) Anfragen zu den Angeboten und Datenschutzerklärungen des NDR

Etwa 50 Zuschriften von Nutzer*innen, Hörer*innen und Zuschauer*innen zu den vom NDR verantworteten Angeboten und den Datenschutzerklärungen bzw. den in den Telemedienangeboten benutzten Tools haben den Rundfunk-

datenschutzbeauftragten im Berichtsjahr erreicht. Die Anliegen waren sehr unterschiedlich:

- Nachfragen zu Datenschutzbestimmungen der Quizz-App
- Sind Nutzungsmessungen (noch immer) erlaubt?
- Einwilligungserfordernisse nach dem TTDSG?
- Generelle Fragen bei der Nutzung der Tagesschau-App und der Verwendung von Cookies
- Datenschutz bei der Verbreitung von Programminhalten über Drittplattformen
- Datenübertragungen bei Push-Mitteilungen
- Datenweitergabe bei Nutzung von Serverdiensten
- Unzulässige Einsehbarkeit von Patientendaten bei Visite?
- Abbildung von personenbezogenen Daten in Dokumentationen
- Anfragen zu Verwendung sogenannten Zähl-Pixeln bei tagesschau.de
- „Deutschland spricht“: Vermeintlich fehlende/nicht-auffindbare Datenschutzhinweise
- Wissenschaftliche Anfrage zum Einsatz von Social PlugIns
- Wissenschaftliche Anfrage zur Nutzung von Clouddiensten von kritischen Infrastrukturen
- Zulässige Verbreitung personenbezogener Daten in den Tagesthemen?
- Verschlüsselung von E-Mail-Newslettern
- Datenschutz und Programmbeschwerden
- Gestaltung der Abfrage von Daten für die Teilnahme an Gewinnspielen

Hinsichtlich des Versands von elektronischen Newslettern wurde moniert, dass die per E-Mail ausgesandten Newsletter des NDR nicht verschlüsselt seien. Der Sachverhalt war zutreffend erfasst. Bis Mitte September 2021 wurden die Newsletter ohne Transportverschlüsselung ausgesandt. Datenschutzrechtlich war deshalb aber nicht im Wege einer aufsichtsrechtlichen Maßnahme eine Verschlüsselung anzuordnen, weil nicht jede E-Mail verschlüsselt werden muss. Eine entsprechende Verpflichtung ergibt sich aus datenschutz-

rechtlichen Vorgaben nicht. Ob und welche Verschlüsselung vorgenommen werden muss, richtet sich vielmehr nach dem Schutzbedarf der in der E-Mail enthaltenen Daten.

Die Newsletter des NDR enthalten programmbezogene Informationen, die zum Beispiel Sendetermine, Ausblicke auf künftige Sendungen und weitere Informationen zu Sendungsinhalten zur Verfügung stellen. Dies sind allesamt Inhalte, die für die Öffentlichkeit bestimmt und daher nicht schützenswert sind und in den Programmangeboten des NDR ebenfalls abgerufen werden können. Auf eine Transportverschlüsslung kann daher verzichtet werden, wenn nach Art. 32 DSGVO ein angemessenes Schutzniveau nicht zwingend zu gewährleisten ist. Da die in den Newslettern übersandten Inhalte keinen Austausch sensibler oder schützenswerter Informationen aufweisen, muss eine Transportverschlüsselung nicht vorgenommen werden. Die für den Versand des Newsletters gespeicherten E-Mail-Adressen liegen zudem auf sicheren Servern des NDR, sind nicht über das Internet für unbefugte Dritte zugänglich und werden mit den üblichen Maßnahmen gesichert. Nunmehr hat sich der NDR aber gleichwohl dazu entschlossen, eine Transport-Verschlüsselung mittels TLS für die Newsletter vorzunehmen.

Viele Anfragen betrafen insbesondere **Berichterstattungen, Dokumentationen, aber auch fiktionale Angebote** des NDR (Kandidatencheck zur Bürgerschaftswahl, Tagesschau, Tagesthemen, Großstadtrevier, Kriminalberichterstattungen, Nordreportagen, „7 Tage …“), in denen Personen kenntlich zu sehen waren. Die Beiträge bzw. einzelne in diesen benannte Passagen wurden geprüft. Maßstab ist für die Verbreitung von (bewegten) Bildern durch Medien die Entscheidung des BGH mit Urteil vom 7. Juli 2020 (Az. VI ZR 250/19) aufgestellt hat (s. o. B. II. 2):

„Die Zulässigkeit von Bildveröffentlichungen ist nach der gefestigten Rechtsprechung des erkennenden Senats nach dem abgestuften Schutzkonzept der §§ 22, 23 KUG zu beurteilen […], das sowohl mit verfassungsrechtlichen Vorgaben (vgl. BVerfGE 120, 180, 211) als auch mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte im Einklang steht (vgl. EGMR, NJW 2012, 1053 Rn. 114 ff.). Danach dürfen Bildnisse einer Person grundsätz-

lich nur mit deren Einwilligung verbreitet werden (§ 22 Satz 1 KUG). Die Veröffentlichung des Bildes einer Person begründet grundsätzlich eine rechtfertigungsbedürftige Beschränkung ihres allgemeinen Persönlichkeitsrechts [...]. Die nicht von der Einwilligung des Abgebildeten gedeckte Verbreitung seines Bildes ist nur zulässig, wenn dieses Bild dem Bereich der Zeitgeschichte oder einem der weiteren Ausnahmetatbestände des § 23 Abs. 1 KUG positiv zuzuordnen ist und berechtigte Interessen des Abgebildeten nicht verletzt werden (§ 23 Abs. 2 KUG). Dabei ist schon bei der Beurteilung, ob ein Bild dem Bereich der Zeitgeschichte zuzuordnen ist, eine Abwägung zwischen den Rechten des Abgebildeten aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK einerseits und den Rechten der Presse aus Art. 5 Abs. 1 GG, Art. 10 EMRK andererseits vorzunehmen [...].

Der Anwendbarkeit der §§ 22, 23 KUG steht im hier betroffenen journalistischen Bereich die zwischenzeitlich eingetretene Geltung der [...] DSGVO schon deshalb nicht entgegen, weil aufgrund der Öffnungsklausel des Art. 85 DSGVO Datenverarbeitungen zu journalistischen Zwecken durch die Anbieter von Telemedien von den die Rechtmäßigkeit der Datenverarbeitung betreffenden Vorschriften in Art. 6 und Art. 7 DSGVO durch nationale Regelungen ausgenommen worden sind (§ 1 Abs. 1 Hs. 2, § 57 Abs. 1 Satz 4 des Staatsvertrags für Rundfunk und Telemedien [Rundfunkstaatsvertrag - RStV] in der seit dem 25. Mai 2018 geltenden Fassung) und die §§ 22, 23 KUG im Hinblick auf die Beurteilung der Zulässigkeit von Bildveröffentlichungen im journalistischen Bereich als die Öffnungsklausel des Art. 85 DSGVO ausfüllende Gesetze anzusehen sind [...]."

Danach gilt also, dass zwischen dem Persönlichkeitsrecht von abgebildeten Personen und dem Berichterstattungsinteresse von Medien eine Abwägung vorgenommen werden muss. Der BGH hat in der Entscheidung die Kriterien benannt, nach denen eine solche Abwägung vorzunehmen ist:

„Maßgebend für die Frage, ob es sich um ein Bildnis aus dem Bereich der Zeitgeschichte handelt, ist der Begriff des Zeitgeschehens. Dieser darf nicht zu eng verstanden werden. Im Hinblick auf den Informationsbedarf der Öffentlichkeit umfasst er nicht nur Vorgänge von historisch-politischer Bedeu-

tung, sondern ganz allgemein das Geschehen der Zeit, also alle Fragen von allgemeinem gesellschaftlichem Interesse. Er wird mithin vom Interesse der Öffentlichkeit bestimmt [...].

Es gehört zum Kern der Presse- und Meinungsfreiheit, dass die Medien im Grundsatz nach ihren eigenen publizistischen Kriterien entscheiden können, was sie des öffentlichen Interesses für wert halten und was nicht. Auch unterhaltende Beiträge, etwa über das Privat- und Alltagsleben prominenter Personen, nehmen grundsätzlich an diesem Schutz teil, ohne dass dieser von der Eigenart oder dem Niveau des jeweiligen Beitrags oder des Presseerzeugnisses abhängt. Gerade prominente Personen können der Allgemeinheit Möglichkeiten der Orientierung bei eigenen Lebensentwürfen bieten sowie Leitbild- und Kontrastfunktionen erfüllen. Auch Aspekte aus ihrem Privatleben wie beispielsweise die Normalität ihres Alltagslebens können der Meinungsbildung zu Fragen von allgemeinem Interesse dienen [...].

Ein Informationsinteresse besteht jedoch nicht schrankenlos, vielmehr wird der Einbruch in die persönliche Sphäre des Abgebildeten durch den Grundsatz der Verhältnismäßigkeit begrenzt [...]. Nicht alles, wofür sich Menschen aus Langeweile, Neugier und Sensationslust interessieren, rechtfertigt dessen visuelle Darstellung in der breiten Medienöffentlichkeit. Wo konkret die Grenze für das berechtigte Informationsinteresse der Öffentlichkeit an der aktuellen Berichterstattung zu ziehen ist, lässt sich nur unter Berücksichtigung der jeweiligen Umstände des Einzelfalls entscheiden [...].

Es bedarf mithin einer abwägenden Berücksichtigung der kollidierenden Rechtspositionen. Die Belange der Medien sind dabei in einen möglichst schonenden Ausgleich mit dem allgemeinen Persönlichkeitsrecht des von einer Berichterstattung Betroffenen zu bringen [...].

Im Rahmen der Abwägung kommt dem Gegenstand der Berichterstattung maßgebliche Bedeutung zu, wobei der Informationsgehalt einer Bildberichterstattung im Gesamtkontext, in den das Personenbildnis gestellt ist, zu ermitteln ist, insbesondere unter Berücksichtigung der zugehörigen Textberichterstattung [...]. Zu prüfen ist, ob die Medien im konkreten Fall eine Ange-

legenheit von öffentlichem Interesse ernsthaft und sachbezogen erörtern, damit den Informationsanspruch des Publikums erfüllen und zur Bildung der öffentlichen Meinung beitragen oder ob sie lediglich die Neugier der Leser nach privaten Angelegenheiten prominenter Personen befriedigen [...]. Je größer der Informationswert für die Öffentlichkeit ist, desto mehr muss das Schutzinteresse desjenigen, über den informiert wird, hinter den Informationsbelangen der Öffentlichkeit zurücktreten. Umgekehrt wiegt aber auch der Schutz der Persönlichkeit des Betroffenen umso schwerer, je geringer der Informationswert für die Allgemeinheit ist [...].

Bei der Prüfung der Frage, ob und in welchem Ausmaß die Berichterstattung einen Beitrag zur öffentlichen Meinungsbildung leistet und welcher Informationswert ihr damit beizumessen ist, ist von erheblicher Bedeutung, welche Rolle dem Betroffenen in der Öffentlichkeit zukommt. Der Europäische Gerichtshof für Menschenrechte unterscheidet zwischen Politikern ("politicians/personnes politiques"), sonstigen im öffentlichen Leben oder im Blickpunkt der Öffentlichkeit stehenden Personen ("public figures/personnes publiques") und Privatpersonen ("ordinary person/personne ordinaire"), wobei einer Berichterstattung über letztere engere Grenzen als in Bezug auf den Kreis sonstiger Personen des öffentlichen Lebens gezogen sind und der Schutz der Politiker am schwächsten ist [...].

Das Gewicht der mit der Abbildung verbundenen Beeinträchtigungen des Persönlichkeitsrechts ist erhöht, wenn der Betroffene nach den Umständen, unter denen die Aufnahme gefertigt wurde, typischerweise die berechtigte Erwartung haben durfte, nicht in den Medien abgebildet zu werden, etwa weil er sich in einer durch Privatheit geprägten Situation, insbesondere einem besonders geschützten Raum, aufhielt (BVerfG, NJW 2017, 1376 Rn. 17; BVerfGE 120, 180, 207). Allerdings erfordern Privatheit und die daraus abzuleitende berechtigte Erwartung, nicht in den Medien abgebildet zu werden, nicht notwendig eine durch räumliche Abgeschiedenheit geprägte Situation. Vielmehr können sie auch außerhalb örtlicher Abgeschiedenheit entstehen [...]."

Aus diesen Grundsätzen des BGH folgt, dass in manchen Fällen Einwilligungen eingeholt werden müssen (das kann auch konkludent geschehen, etwa

durch das wissentliche Sprechen in eine Kamera), in anderen Situationen bedarf es für das Aufnehmen und Verbreiten von Personenbildnissen (oder anderen personenbezogenen Daten) keiner Einwilligung, weil das in dem Zitat des Urteils genannte **Medienprivileg** greift, mithin die Abwägung ergibt, dass das Informationsinteresse der Öffentlichkeit höher zu bewerten ist als das Interesse der abgebildeten Personen. Die Darstellung der Entscheidung nimmt deshalb hier einen breiten Raum ein, weil der **Kernbereich der Tätigkeit des NDR betroffen ist und die bereits vorgenommenen und auch zukünftigen Prüfungen der Verletzung der informationellen Selbstbestimmung vorbehaltlich weiterer Entscheidungen an diesen Maßstäben vorgenommen wird**.

d) Anfragen von Redaktionen

Die Mitgliedstaaten sind gemäß Art. 85 Abs. 1 DSGVO aufgefordert, den Schutz personenbezogener Daten und das Recht auf freie Meinungsäußerung und Informationsfreiheit durch nationale Rechtsvorschriften in Einklang zu bringen. Entsprechend der sogenannten Öffnungsklausel des Art. 85 Abs. 2 DSGVO werden die Mitgliedsstaaten ermächtigt, unter anderem zu journalistischen Zwecken Abweichungen und Ausnahmen von Kapiteln, also bestimmten Vorschriften, der Datenschutzgrundverordnung vorzusehen, soweit dies erforderlich ist, um einen Einklang der Interessen von Datenschutz und Berichterstattungen herbeizuführen. Derartige Regelungen, die Abweichungen von datenschutzrechtlichen Vorgaben für den journalistischen Bereich erlauben, werden als Medienprivileg bezeichnet. Die Privilegierung besteht also insofern, als bestimmte Vorgaben der DSGVO bereichsspezifisch für journalistische Zwecke nicht in Gänze oder nur teilweise gelten (zum Beispiel hinsichtlich des Erfordernisses der Einholung von Einwilligungen, s. die obigen Ausführungen). Manche datenschutzrechtliche Vorschriften gelten aber auch für die redaktionelle Arbeit, weshalb es regelmäßig Beratungsbedarf von den Redaktionen an den Rundfunkdatenschutzbeauftragten herangetragen werden. Dabei geht es überwiegend um Fragen der Transparenz und der Datensparsamkeit hinsichtlich der Verarbeitung von Daten von Nutzer*innen, Hörer*innen und Zuschauer*innen, aber auch um organisatorische Belange:

- „Wünsch Dir Deinen NDR“ – Gestaltung und Verwendung von Formularen und Daten zur Publikumsaktion
- Anfragen zur etwaig weiteren Nutzung von Kundenkontaktdaten
- Nutzungen von eingesandten Bildern vom Publikum
- Redaktionelle Auswertung von Nutzer*innen-Kommentaren
- Ergänzende Datenschutzhinweise für „Deutschland spricht 2021“
- ARD Quizz App: Gästeaccounts, Messenger-Dienste, Gewinnspielregeln
- Zuschauerinnenbefragungen durch die NDR Sportzone
- Rekrutierung von Teilnehmer*innen für Medienforschungsstudien
- Datenschutzbestimmungen für die Teilnahme am ESC
- Besucher*innendaten beim Gästemanagement
- Virtuelle Besucherführungen
- Anfragen zum Direktversand von Preisen an Gewinner*innen
- Datenverarbeitungen im Zuge der „Wahlarenen“ vor der Bundestagswahl
- Umgang mit Zuschriften aufgrund einer Programmaktion mit der Deutschen Depressionshilfe
- Weitergabe von Daten an die Polizei
- Redaktionelles Arbeiten im Homeoffice
- Entsorgung von Datenträgern

Die Anfragen wurden bearbeitet und die Beratungsergebnisse entsprechend vom NDR umgesetzt.

e) Beteiligungsunternehmen des NDR

Aufgrund des Hinweises des Rundfunkdatenschutzbeauftragten des NDR wurden die Cookie-Banner der Beteiligungsunternehmen des NDR angepasst. Wie so oft wurde auf den Internetseiten ein Banner eingesetzt, mit dem mittels Nudging versucht wurde, die Nutzer*innen zu weniger datenschutzfreundlichen Einstellungen zu bewegen. Dies geschieht durch das Vorspiegeln der Wahl der vermeintlich datenschutzfreundlichsten Variante durch farblich oder dunkel hinterlegte Felder – also eine Farbwahl, die die Aufmerk-

samkeit anzieht –, während tatsächlich beim Anklicken dieses Buttons Gegenteiliges geschieht. Dies wurde nun behoben.

3. Rundfunkteilnehmerdatenschutz

Aktuelle Fragen und Themen bezüglich des Rundfunkteilnehmerdatenschutzes werden regelmäßig im AKDSB erörtert. Es besteht daher ein enger Kontakt mit der Datenschutzbeauftragten des Beitragsservice. An den Beitragsservice haben sich im Jahr 2021 6.888 Personen gewandt und erfragt, welche personenbezogenen Daten über sie verarbeitet werden. Von diesen Auskunftsersuchen entfielen 1.116 auf den NDR (im Jahr 2020 sind insgesamt 33.379 Auskünfte vom Beitragsservice erteilt worden, davon 4.997 für den NDR). Ein deutlicher Rückgang.

Beim NDR stellt sich die Situation wie folgt dar: Auskunftsanfragen gemäß Art. 15 DSGVO, die den gesamten NDR betrafen, wurden vierzehnmal eingereicht. Alle Anfragen konnten aufgrund hinreichender Identifizierung beantwortet werden. Überdies gab es weitere 24 Anträge auf Auskunft, die nur den Rundfunkbeitragseinzug betrafen.

Als Verantwortlicher im Sinne der Datenschutzgrundverordnung ist der NDR für die Bearbeitung der Anfragen und die Erfüllung des Anspruches zuständig. Auch diese Anfragen konnten beantwortet werden. Insgesamt ist die Anzahl der Anfragen stabil.

20 Personen haben Beschwerden an den Rundfunkdatenschutzbeauftragten gerichtet (teils mit mehrfachen Eingaben). Vorgetragen wurde regelmäßig,

- eine Auskunft sei nicht erteilt worden,
- die Frist zur Beauskunftung sei nicht eingehalten worden oder
- die Auskunft sei unvollständig.

Die Prüfung hat aber regelmäßig ergeben, dass keine Datenschutzverletzungen vorlagen. Hinsichtlich weiterer Zuschriften aufgrund behaupteter unzulässiger oder stark gehäufter Nachfragen des Beitragsservice zu Rundfunkbeitragspflichten war festzustellen, dass der Regelungsgehalt des **§ 8 Rundfunkbeitragsstaatsver-**

trag oft unbekannt war. In dieser Vorschrift ist geregelt, welche Daten zum Zwecke des Beitragseinzugs verarbeitet werden dürfen. Weiterhin ist dort auch geregelt, dass nicht die Rundfunkanstalten bzw. der Beitragsservice die Daten „herausfinden“ müssen (aber können), sondern dass Beitragspflichtige selbst die Daten ohne weitere Aufforderung zu übermitteln haben. Das Innehaben einer Wohnung, einer Betriebsstätte oder eines beitragspflichtigen Kraftfahrzeugs ist also qua Gesetz unverzüglich schriftlich der zuständigen Landesrundfunkanstalt anzuzeigen (sog. Anmeldung). Dies gilt auch für die Änderung einer Anschrift (sog. Änderungsmeldung).

4. Beschäftigtendatenschutz

Der Beschäftigtendatenschutz hat auch im Jahr 2021 eine große Rolle gespielt und wird dies voraussichtlich auch weiterhin tun. Im Schwerpunkt ging es um Systeme, mit denen einzelne Bereiche oder die gesamte Belegschaft miteinander arbeiten.

a) Kollaborationssysteme

Kollaborationssysteme sind elektronische Anwendungen und Plattformen, mit denen grundsätzlich eine nicht ortsgebundene Kommunikation und Zusammenarbeit ermöglicht werden kann. Solche Systeme gab es schon lange. In pandemischen Zeiten (weitgehend) ohne Dienstreisen und mit Abstandsgeboten ist der Bedarf an derartigen Anwendungen gestiegen.

Zur Erfüllung dieser Bedarfe hatte der NDR zunächst noch beabsichtigt, eine Mischung aus Angeboten (amerikanischer) Großkonzerne und den Einsatz von Open-Source-Software bereitzustellen. Von diesem Ansatz ist der NDR allerdings immer weiter abgerückt. Eine Reihe von digitalen Anwendungen und Werkzeugen für die sogenannte „Collaboration“ wird von einem Anbieter bereitgestellt werden. Datenschutzrechtlich entstehen dadurch eine Reihe von Problemen und ein starker Befassungsaufwand (so müssen beispielsweise alle Standardkonfigurationen in den Blick genommen werden). Mehrfach wurde (u. a. auch von der RDSK) darauf hingewiesen, dass bei der zentralen Anwendung – einem Videokonferenzsystem – der Eigenbetrieb eines solchen Sys-

tems (mit weiteren - vorgelagerten und anhängenden – Services und Funktionen) datenschutzrechtlich vorzugswürdig ist. Denn die Datenhaltung bleibt allein beim Verantwortlichen (oder gemeinsam bei mehreren Verantwortlichen). Dies hat den Vorteil, dass die Verarbeitungsprozesse weitgehend selbst gesteuert werden können. Auch die Konfigurationen, der Betrieb und die Wartung können (weitgehend) eigenständig vom Verantwortlichen vorgenommen und gesteuert werden.

Im Laufe des Jahres 2021 hat sich nun aber auch der NDR von diesem Modell verabschiedet und das eigens betriebene System ersetzt durch einen externen Dienstleister. Das bedeutet, dass die Daten einem Dritten unter Rückgriff auf dessen Ressourcen und Expertise anvertraut werden müssen. Erforderlich werden daher vertragliche Vereinbarungen mit dem Dienstleister, der als Auftragsverarbeiter bezeichnet wird. Nach Art. 4 Abs. 8 DSGVO muss der NDR eine entsprechende Vereinbarung gemäß Art. 28 Abs. 3 DSGVO schließen und sich in dieser die datenschutzrechtlichen Anforderungen zusichern lassen. Zu den einzelnen datenschutzrechtlichen Anforderungen gehört derzeit auch, dass die Entscheidung des Europäischen Gerichtshofs (EuGH) zur Übermittlung personenbezogener Daten in Drittländer vom 16. Juli 2020 (Rs. C-311/18 – sog. Schrems II) berücksichtigt werden muss, weil entsprechende Systeme häufig personenbezogene Daten auch in den USA verarbeiten. Der EuGH hatte allerdings – bis heute gültig – festgestellt, dass die bisherigen Abkommen für die Übermittlung personenbezogener Daten in Drittländer unwirksam sind, weil die Zugriffsmöglichkeiten der US-Behörden nach den US-Gesetzen das nach EU-Recht akzeptable Maß übersteigen. Zwar werden nun vermehrt von den amerikanischen Anbietern Garantien abgegeben, um das rechtliche Vakuum zu kompensieren. Insgesamt bleiben aber noch viele Fragen offen, so dass es letztlich zum Einsatz von mehreren Systemen gekommen ist.

Kollaborationsmittel erschöpfen sich nicht in Videokonferenzsystemen. Neben diesen Systemen werden weitere Anwendungen (Planungstools, Messenger-Dienste, Tools, mit dem Wahlen und Abstimmungen durchgeführt werden und weitere unterstützende und ergänzende Anwendungen für die tägliche Arbeit benötigt. Auch wenn sie im Rahmen einer „Software as a Service“ von

einem Unternehmen bereitgestellt werden, ist für alle Dienste eine eigenständige Prüfung notwendig, um die Verarbeitung von personenbezogenen Daten einschätzen zu können.

b) Kontaktnachverfolgung in der Pandemie

Die andauernde pandemische Lage hatte auch Einfluss auf den Beschäftigtendatenschutz. Im Kern ging es darum, die in den Eindämmungsverordnungen der Länder vorgesehenen Maßnahmen im NDR umzusetzen. So hat der NDR eine Kontaktnachverfolgungs-App gesucht, um beispielsweise für Kantinenbesuche oder Live-Veranstaltungen digitale Kontaktnachverfolgungen zu ermöglichen. Empfohlen wurde dazu die „Corona-Warn-App“, die der Anbieter, das Robert-Koch-Institut (RKI), um eine entsprechende Funktion ergänzt hatte. Dem Vorzug galt dieser App, weil Alternativen zumindest über längere Strecken immer neue Schwachstellen aufwiesen: So konnten etwa bei einem Anbieter auch mit abfotografierten und im Internet verbreiteten QR-Codes Check-Ins vorgenommen werden, obwohl die sich registrierenden Personen tatsächlich nicht anwesend waren. Der Chaos Computer Club e. V. forderte hinsichtlich der Luca-App sogar eine „Bundesnotbremse“, weil er die Sicherheitsmängel der App als schwer einschätzte (www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse). Der NDR war jedenfalls der Empfehlung seines Rundfunkdatenschutzbeauftragten erfolgt, die Corona-Warn-App einzusetzen, so dass keine Probleme auftraten.

c) Corona-Tests, Testergebnisse, Impf- und Genesungsstatus

Gesundheitsdaten zählen zu sensiblen und besonders schützenswerten Daten. Entsprechend sind solche Angaben in einem Beschäftigungsverhältnis auch nur nach gesetzlichen Anforderungen und mit großer Umsicht zu verarbeiten.

Im Jahr 2021 war der Umgang mit Corona-Tests und Testergebnissen bereits weitgehend eingeübt und die diesbezüglichen Anfragen und Beschwerden rückläufig.

Zum September 2021 hatte der Bundesgesetzgeber die SARS-CoV-2-Arbeitsschutzverordnung geändert und ergänzt. Darin hieß es nunmehr:

„Bei der Festlegung und der Umsetzung der Maßnahmen des betrieblichen Infektionsschutzes kann der Arbeitgeber einen ihm bekannten Impf- oder Genesungsstatus der Beschäftigten berücksichtigen."

Arbeitgeber hatten nun neben den bekannten und weiterhin geltenden Maßnahmen zur Eindämmung der Corona-Pandemie die Möglichkeit, bei der Gestaltung der Arbeitsplätze und betrieblichen Abläufe zusätzlich diese Kenntnisse heranzuziehen. Da sich der Gesetzgeber allerdings (zunächst) nicht für eine Auskunftspflicht der Beschäftigten entschlossen hatte, war es möglich im Rahmen der Freiwilligkeit anzufragen, wie es um den Impf- oder Genesungsstatus bestellt ist. Wie derartige Fragen gestellt und die Ergebnisse verwendet werden dürfen, wurde jedenfalls **für den NDR datenschutzrechtlich geklärt und ein entsprechendes Formular zur Verfügung** gestellt. Zu beachten war insbesondere, dass niemanden Nachteile erwachsen dürfen, wenn keine Angaben dazu gemacht werden.

Zu einer entsprechenden freiwilligen Abfrage kam es allerdings nicht mehr. Überholt wurde die Entwicklung durch eine Änderung des Infektionsschutzgesetzes. Am 24. November 2021 wurde mit § 28 b) Infektionsschutzgesetz die Pflicht eingeführt, dass in Unternehmen bei Betreten der Arbeitsstätte ein Impf- und Genesenennachweis oder eine aktuelle Bescheinigung über einen negativen Coronatest mitzuführen ist. Zugleich muss der Arbeitgeber kontrollieren, ob die Beschäftigten dieser Verpflichtung nachkommen und diese Kontrollen dokumentieren. Auch wenn die Prüfungen an den einzelnen Standorten des NDR unterschiedlich durchgeführt wurden, gab es die Verständigung auf die Erhebung des vollständigen Namens, der Personalnummer (um Identitätsverwechselungen bei gleichlautenden Namen auszuschließen) und die Erfassung des nachgewiesenen Status. Die Daten werden für längstens sechs Monate gespeichert (§ 28 b) Abs. 3 Ziffer 2 Infektionsschutzgesetz).

Weitere Fragen in diesem Zusammenhang stellten sich bezüglich der **Geltendmachung von Entschädigungsansprüchen**: In manchen Fällen können Arbeitgeber Entschädigungsansprüche gegenüber Behörden geltend machen, wenn es zu Arbeitsausfällen gekommen ist, die nicht vermeidbar waren. Zur Prüfung der Voraussetzungen verlangen die Behörden Nachweise auch über den Impf- und Genesungsstatus betroffenen Personen. Hier galt es, die entsprechenden Voraussetzungen (des Infektionsschutzgesetzes) bzw. die Rechtsgrundlagen für eine Datenübermittlung zutreffend auszulegen.

Diesbezüglich ist gerichtlich die Abfrage des Impf- bzw. Genesungsstatus allerdings bislang noch nicht geklärt. Von der datenschutzrechtlichen Aufsichtsbehörde des NDR wird – vorbehaltlich einer anderslautenden rechtskräftigen Entscheidung eines Gerichts – davon ausgegangen, dass der Arbeitgeber ein entsprechenden Fragerecht auch im Zusammenhang mit Entschädigungen wegen einer Absonderung, Quarantäne oder einem Tätigkeitsverbot nach § 56 IfSG hat. Dies ergibt sich aus folgenden Erwägungen:

Als Gesundheitsdatum unterfällt der Impfstatus von Beschäftigten Art. 9 Abs. 1 DSGVO. Der Arbeitgeber darf solche Daten nach § 26 Abs. 3 BDSG nur dann verarbeiten, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich sind. Zugleich darf kein triftiger Grund zur Annahme bestehen, dass schutzwürdige Interessen der Beschäftigten einer Verarbeitung dieser Informationen durch den Arbeitgeber entgegenstehen.

Nach hiesiger Auffassung hat der Arbeitgeber ein begründetes Interesse an der Feststellung, ob er einer beschäftigten Person, die sich in einem Risikogebiet aufgehalten hat oder Kontakt zu einer erstinfizierten Person hatte, Verdienstausfallentschädigung nach § 56 Abs. 5 S. 1 IfSG zahlen muss, weil sich die beschäftigte Person abzusondern hat. Die Kenntnis des Impfstatus ist damit für den Entschädigungsanspruch der beschäftigten Person und für den Erstattungsanspruch des Arbeitgebers gegenüber den für eine Erstattung zuständigen Behörden maßgeblich (§ 56 Abs. 5 S. 2 und Abs. 12 IfSG). Denn eine Entschädigung ist nicht zu leisten, wenn keine Quarantänepflicht mehr

besteht. Dies ist nach dem RKI dann der Fall, wenn eine Person vollständig geimpft ist.

Eine Impfung gegen Sars-CoV-2 ist eine Schutzimpfung im Sinne des § 56 Abs. 1 S. 4 IfSG. Folglich hat eine beschäftigte Person keinen Anspruch auf eine Entschädigung wegen einer Quarantäne, § 56 Abs. 1 S. 4 IfSG., weil durch eine Impfung eine Quarantäne hätte vermieden werden können.

Sinnhaft ist daher das Fragerecht des Arbeitgebers, weil in einem etwaigen Prozess einer beschäftigten Person diese Klage auf Entschädigung gegen den Arbeitgeber erheben müsste, wenn die Zahlung verweigert wird. Der Impfstatus wäre als Nachweis für den bestehenden Anspruch also geltend zu machen. Auch vor einem etwaigen Klageverfahren ist daher die Information über einen Status mitzuteilen, weil nicht zuerst eine Klage vorgeschaltet werden muss. Zu beachten ist lediglich, dass das zur Verfügung gestellte Formular für eine Abfrage der Mitbestimmung gemäß § 87 Abs. 1 Nr. 1 BetrVG unterliegt.

d) Mobiles Arbeiten, Homeoffice

Die im Jahr 2020 vom NDR erarbeitete und vom Rundfunkdatenschutzbeauftragten mitberatende **Dienstvereinbarung zum Homeoffice** wurde nicht in Kraft gesetzt. Dies ist misslich, da in dieser Vereinbarung eine Reihe von Vorgaben zum Arbeiten in häuslicher Umgebung geregelt werden sollten. Gemeinsam mit dem IT-Sicherheitsbeauftragten des NDR wurden neue Entwürfe für Regelungen unterbreitet, damit das erforderliche Sicherheitsniveau gewährleistet wird. Es soll damit sichergestellt werden, dass die Regelungen zum Datenschutz und zur IT-Sicherheit auch für das regelmäßige und nicht regelmäßige mobile Arbeiten gelten. Neben weiteren einzelnen Regelungen werden auch Vorgaben gemacht, wie mit einem etwaigen Einsatz von privaten Geräten für dienstliche Zwecke umzugehen ist. Diese Vorgaben sind vom NDR mit Priorität umzusetzen, weil viele über das offene Internet zu erreichende Anwendungen aufgrund einer etwaigen privaten Nutzung ebenso sicher sein müssen, wie im Falle einer Verwendung dienstlicher Endgeräte.

Videokonferenzen dienten noch immer als Ersatz für Sitzungen, die sonst in Präsenz durchgeführt wurden. Grundsätzlich gilt: In einer Abteilung kann die/der Vorgesetzte Sitzungen und Videokonferenzen anberaumen, weil sie/er insoweit die Organisationshoheit für den jeweiligen Bereich hat. An den im NDR eingerichteten Arbeitsplätzen können Vorgesetzte daher Videokonferenzen anberaumen, ebenso wie dies bei Präsenzsitzungen der Fall war. Anders stellte sich die Situation teilweise noch im Homeoffice dar: Mit den im NDR ursprünglich genutzten Konferenzsystem war es nicht möglich, den Hintergrund des gesendeten Bildes auszublenden, so dass lediglich die teilnehmenden Personen zu sehen waren. Auch existiert im NDR keine Regelung (etwa in Form einer Betriebsvereinbarung), wonach es den Beschäftigten vorgegeben ist, das Bild zwingend aus dem heimischen Büro zu senden. Weiterhin sind die Regelungen der Teleheimarbeit nicht auf die derzeitigen Vorgaben zum Homeoffice anwendbar. Wenn daher Videokonferenzen aus dem Homeoffice heraus durchgeführt wurden, war den Teilnehmenden zu gewähren, auch ohne aktive Videokamera oder nur per Telefon an einer Konferenz teilzunehmen. Sofern Zweifel an einer Teilnahme an einer Konferenz bestanden, konnten diese ausgeräumt werden durch die Anzeige der Liste der Teilnehmenden am Bildschirm.

e) Weitere Tätigkeiten im Zusammenhang mit der Corona-Pandemie

Die Olympischen Spiele in Tokio waren nicht nur aufgrund der pandemischen Lage in Japan herausfordernd. Auch die Einreise- und Akkreditierungsanforderungen waren aus datenschutzrechtlicher Sicht problematisch. Die Veranstalter hatten dazu in einem sogenannten „Playbook“ diverse Auflagen vorgeschrieben, um die weitere Ausbreitung des Virus durch die zahlreichen ausländischen Gäste einzudämmen. Die Vorgaben für die Einreise und den Aufenthalt in Japan waren deutlich strenger als die hiesigen Regelungen zur Eindämmung der Pandemie, sowohl hinsichtlich der geforderten Offenlegung von Gesundheitsdaten als auch bezüglich des Trackings von Aufenthalten von Personen (mittels GPS). Auch wurden Beförderungen mit bestimmten Verkehrsmitteln und Aufenthaltsorte für Journalist*innen vorgegeben. Letztlich wurden die Mitarbeiter*innen des NDR durch Information und Transparenz für die Risiken ihrer Rechte auf informationelle Selbstbestimmung sensibili-

siert, da kein Einfluss auf die Vorgaben genommen werden konnte. Insgesamt (nicht beim NDR) wurden rund 15 Prozent der Akkreditierungen für deutsche Medien zurückgegeben. Dies ist eine ungewöhnlich hohe Zahl, die auf die starken Bewegungsbeschränkungen und Überwachungen zurückzuführen ist (www.deutschlandfunk.de/olympische-spiele-2021-warum-viele-medien-nicht-in-tokio.2907.de.html?dram:article_id=498145).

f) Mobilität

Die Mobilität der Beschäftigten wird immer mehr geprägt durch die Nutzung von Fahrrädern, E-Bikes, Ride-Sharing-Services, klassischen Taxis. Daher hat der NDR Vereinbarungen mit entsprechenden Anbietern, z. B. von Radleasing-Unternehmen, geschlossen. Naturgemäß fallen bei der Nutzung derartiger Dienste personenbezogene Daten an (Namen, Standortdaten, Abrechnungsdaten, aber auch – aus ergonomischen Gründen etwa beim Radleasing – Daten über das Gewicht und die Körpergröße). Hinsichtlich der einzelnen Fragen aber auch zu den Angeboten insgesamt entfaltet sich daher regelmäßiger Beratungsbedarf zu den Datenverarbeitungen, der zügig bearbeitet werden konnte.

g) Schulungen

Wie in den Jahren zuvor auch, wurden datenschutzrechtlich Schulungen für die neuen Auszubildenden im technischen Bereich und neue Volontär*innen durchgeführt. Zudem wird es ergänzend für alle Beschäftigten auch Online-Schulungen geben. Diese sollen aber zukünftige persönliche Schulungs- und Informationsveranstaltungen nicht ersetzen, sondern ergänzen. Denn eine Schulung einzelner Bereiche, die gezielt auf die besonderen Bedarfe unter Berücksichtigung der regelmäßig benutzten IT-Anwendungen eingeht, erhöht das datenschutzrechtliche Niveau, sorgt für mehr Sensibilität und beugt dem Einsatz von nicht geprüften und vom NDR nicht freigebenden Anwendungen vor (sog. „Schatten-IT“). Die bereits vom Rundfunkdatenschutzbeauftragten des NDR angeregte Erarbeitung eines umfassenden Schulungskonzepts und weitere organisatorische Maßnahmen zur Erhöhung der Sensibilität (z. B. durch

geeignete (digitale) Veröffentlichungen) wurden allerdings bislang nicht aufgegriffen bzw. nur sind nur in einigen Bereichen des NDR in Klärung.

h) Datenverarbeitung in Personalvertretungen des NDR

Zu klären war die an den Rundfunkdatenschutzbeauftragten adressierte Frage, ob die (örtlichen) Schwerbehindertenvertretungen aus Kapazitätsgründen auch über den eigenen Einsatzort hinaus tätig werden dürfen, um die Arbeitsbelastung von einer anderen oder der Gesamt- Schwerbehindertenvertretung zu kompensieren. Der NDR hatte ein entsprechendes Begehren abgelehnt, weil dies den gesetzlichen Vorgaben und der im NDR geltenden Vereinbarung widerspräche.

Die Prüfung ergab, dass das Vorgehen des NDR nicht zu beanstanden war. Denn zum einen ist der Wortlaut des einschlägigen Gesetzes eindeutig. Nur unter den Voraussetzungen des § 180 Abs. 6 S. 1 SGB IX kann eine Gesamtschwerbehindertenvertretung eine Ersatzzuständigkeit erlangen:

„Die Gesamtschwerbehindertenvertretung vertritt die Interessen der schwerbehinderten Menschen in Angelegenheiten, die das Gesamtunternehmen oder mehrere Betriebe oder Dienststellen des Arbeitgebers betreffen und von den Schwerbehindertenvertretungen der einzelnen Betriebe oder Dienststellen nicht geregelt werden können, sowie die Interessen der schwerbehinderten Menschen, die in einem Betrieb oder einer Dienststelle tätig sind, für die eine Schwerbehindertenvertretung nicht gewählt ist; dies umfasst auch Verhandlungen und den Abschluss entsprechender Inklusionsvereinbarungen.“

Zum anderen besteht eine betriebliche Integrationsvereinbarung im NDR, die wirksam den Umgang mit personenbezogenen Daten regelt (Art. 88 Abs. 1 DSGVO i. V. m. ErwGr 155). In dieser sind explizit die Aufgaben der örtlichen Schwerbehindertenvertretungen festgeschrieben. Ein Zuständigkeits- oder Regelungsdefizit besteht im NDR daher nicht derart, dass die Gesamtschwerbehindertenvertretung an die Stelle einer örtlichen Vertretung treten müsste. Auch in der Rechtsprechung wird unter Bezugnahme auf die soeben zitierte Norm (bzw. der insoweit inhaltsgleichen vorherigen Regelung) stets darauf

verwiesen, dass es bei der Aufgabenverteilung zwischen örtlicher und überörtlicher Schwerbehindertenvertretung nach den Regelungen des SGB IX verbleibt, wenn solche eingerichtet sind. Die Ersatzzuständigkeit einer Gesamtschwerbehindertenvertretung entfaltet sich nur dann, wenn eine örtliche Schwerbehindertenvertretung nicht gewählt ist (BAG, Urteil vom 04.11.2015, 7 ABR 62/13, BAG, Urteil vom 28.7.1983, 2 AZR 122/82, ArbG Darmstadt, Urteil vom 14.11.2017 - 9 Ca 249/17). Die Ablehnung des Begehrens durch den NDR war daher nicht zu beanstanden.

Weitere Anfragen betrafen Folgen aus dem neu gefassten NDR Staatsvertrag. § 41 Abs. 3 NDR Staatsvertrag lautet seit September 2021 wie folgt:

„Arbeitnehmerähnliche Personen im Sinne des § 12a Tarifvertragsgesetz gelten als Beschäftigte im Sinne des § 4 Absatz 3 Bundespersonalvertretungsgesetzes. Für sie gelten die gleichen Personalvertretungsrechte wie für Beschäftigte, soweit ihr Vertrag mit dem NDR entsprechende Verpflichtungen enthält und die gesetzlichen Vorgaben Anwendung finden können."

Die Begründung des Gesetzgebers dazu lautet:

„Einbeziehung der festen Freien-Mitarbeiter in Regelungen zum Personalvertretungsrecht: Die bestehende Regelung des NDR-StV zur Personalvertretung gilt nicht für die festen Freien-Mitarbeiter. Der Staatsvertragsentwurf sieht vor, dass für feste Freie-Mitarbeiter des NDR nunmehr die gleichen Personalvertretungsrechte wie für Beschäftigte gelten. Die Änderung findet sich in § 41 Absatz 3 NDR-StV-E. Danach gelten arbeitnehmerähnliche Personen im Sinne des § 12 a Tarifvertragsgesetz als Beschäftigte im Sinne des § 4 Absatz 3 Bundespersonalvertretungsgesetzes."

Zu klären war daher die Frage, welche **Datenkategorien von freien Mitarbeiter*innen** an die Personalvertretungen und Gewerkschaften zur Wahrnehmung ihrer Aufgaben übermittelt werden dürfen (etwa Laufzeiten von Rahmenverträgen, die Gesamtbeschäftigungsdauern). Dies ergibt sich aus den Zuständigkeiten der Personalvertretungen nach dem Bundespersonalvertretungsgesetz oder aufgrund einer Betriebsvereinbarung zwischen dem NDR

und den Personalvertretungen (die allerdings noch nicht geschaffen war). Jedenfalls war darauf hinzuweisen, zu welchem Zweck die Daten generell und regelmäßig benötigt werden für die von Personalvertretungen zu erledigenden Aufgaben (nach den Prinzipien der Zweckbindung und Datensparsamkeit).

i) E-Mail-Werbung durch Gewerkschaften

Einigen Unmut und besorgte Nachfragen erzeugte eine an alle Beschäftigten des NDR ausgesandte E-Mail von einem Gewerkschaftsmitglied, das selbst nicht im NDR beschäftigt ist. Die Anfang August 2021 versandte Nachricht enthielt Ausführungen zur Entscheidung des Bundes-verfassungsgerichts bezüglich der Erhöhung des Rundfunkbeitrags. Nach der einschlägigen Rechtsprechung des Bundesarbeitsgerichts (BAG, Urteil vom 20.01.2009 - Aktenzeichen 1 AZR 515/08) gilt zunächst:

„Eine tarifzuständige Gewerkschaft ist aufgrund ihrer verfassungsrechtlich geschützten Betätigungsfreiheit grundsätzlich berechtigt, E-Mails zu Werbezwecken auch ohne Einwilligung des Arbeitgebers und Aufforderung durch die Arbeitnehmer an die betrieblichen E-Mail-Adressen der Beschäftigten zu versenden."

Derartige elektronische Aussendungen sind daher grundsätzlich hinzunehmen, weil die E-Mail von einer im NDR vertretenden Gewerkschaft stammte. Gleichwohl gestaltet sich der Fall aus datenschutzrechtlicher Sicht problematisch, weil der Absender keinen internen Zugriff auf die E-Mail-Adressen haben konnte. In welcher Art und Weise die E-Mail-Adressen an die Gewerkschaft gelangt waren, konnte nicht nachvollzogen werden. Ein Zugriff von außen auf interne Systeme des NDR (das Intranet) wurde nicht erkannt. Es ist daher nicht unwahrscheinlich, dass die E-Mail-Adressen von einer im NDR beschäftigten Person weitergegeben wurden, da alle Beschäftigten einen Zugriff auf das gesamte im Intranet hinterlegte Telefonbuch einschließlich der dort aufgeführten E-Mail-Adressen haben. Möglich ist folglich, dass die E-Mail-Adressen oder auch Gruppenverteiler von dort genommen und an die Gewerkschaft übermittelt wurden. Weil dies aber nicht nachvollziehbar gemacht

werden kann, blieben dies bloße Vermutungen. Auch kann der NDR eine solche Weiterreichung faktisch oder technisch nicht unterbinden, weil alle Beschäftigten aus organisatorischen Gründen und solchen der Gewährleistung betrieblicher Abläufe entsprechende Zugriffe auf die Erreichbarkeiten der im NDR beschäftigten Personen haben müssen.

Einzelne Personen haben ihre Auskunftsrechte gegenüber der Gewerkschaft geltend gemacht, aber gleichwohl die Herkunft der Daten nicht erfahren. Die Art und Weise des Umgangs entspricht nicht den gesetzlichen Vorgaben (Art. 15 DSGVO), weil die Auskunftsersuchen nicht vollständig bearbeitet wurden.

Zu Recht wurde daher auch besorgt von einem Journalist*innenverband angefragt, ob die Daten aus einem Datenleck des NDR stammen. Auch wurde von dem Verband in nachvollziehbarer Weise dargelegt, dass viele Journalistinnen und Journalisten besorgt sind, weil einige ihrer Accounts als sensibel und besonders schützenswert einzustufen sind.

Insgesamt ist der Vorgang datenschutzrechtlich als äußerst kritisch zu bewerten, auch wenn grundsätzlich E-Mails zu Werbezwecken ausgesandt werden dürfen. Denn dies rechtfertigt noch nicht die Übermittlung von derartigen Daten an Dritte (zumal auch private E-Mail-Adressen weitergegeben wurden) und deutet auf eine **mangelhafte Sensibilität** der Person(en) hin, die die Datenweitergabe vorgenommen hat.

j) Datenschutzverletzung bei der BBP

Die Baden-Badener Pensionskasse VVaG (BBP) führt im Auftrag des NDR die Rentenabrechnungen aus. Anfang September 2021 meldete der Datenschutzbeauftragte der BBP eine Datenschutzverletzung derart, dass durch einen technischen Fehler Versorgungsempfänger des NDR versehentlich Verdienstnachweise von anderen Versorgungsempfängern erhalten hätten. Gleichzeitig wurde mitgeteilt, dass das Versehen allein auf einem technischen Fehler beruhte, der gefunden und abgestellt worden sei. Zudem seien die betroffenen Personen bereits informiert worden. Insgesamt stellte sich heraus, dass es sich um einen Ausreißer handelte und sowohl die Fehlerbe-

hebung als auch die Benachrichtigung (Art. 34 DSGVO) unverzüglich erfolgten. Von weiteren Maßnahmen konnte daher aufgrund des Ausnahmecharakters der Sache abgesehen werden.

5. Weitere Beratungen und Prüfungen im NDR

Anfragen zu Digitalisierungs-, Organisations- und Strukturänderungsvorhaben prägen die tägliche Arbeit. In weiten Teilen des NDR erfolgt eine frühzeitige Einbeziehung des Datenschutzes. Betroffen sind fast alle Bereiche des NDR und gerade auch das Beschaffungswesen des NDR fragt Beratungen frühzeitig nach, um datenschutzrechtliche Vorgaben bereits bei Ausschreibungen zu berücksichtigen. Das ist zu begrüßen, denn in der Datenschutzgrundverordnung heißt es u. a.:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen …“

Datenschutz muss also von Anfang an berücksichtigt werden, weil nicht-datenschutzrechtkonforme Anwendungen gar nicht erst beschafft werden dürfen.

a) Organisations- und Strukturprojekte

Datenschutzrechtlich zu betrachten waren u. a.:

- Systeme zur Erstellung, Bearbeitung und Veröffentlichung redaktioneller Inhalte
- Administrationstools
- digitale Styleguide-Portale
- Systeme zur Abwicklung von Unfallmeldungen
- Anwendungen zur Herstellung von Insertierungen
- Umbauten von Nachrichtenstudios

- Nutzerbeziehungsmanagementsysteme (CRM)
- NDR-Datenbankanwendungen
- Genehmigungssysteme für einzelne Programm- und Produktionsvorhaben
- der neue interne Pressespiegel
- Terminbuchungs- und Sachleihe-Tools
- die Nutzung von Cloud-Kapazitäten Dritter
- neue Interview-Tools
- der Ersatz von Unfallmeldesystemen
- Systeme für Insertierungen
- digitale Lernplattformen
- neue interne WiKi-Anwendungen
- unternehmensinterne Text- und Mediensuche-Anwendungen
- Online-Bewerber-Tools
- Speech-to-text-Anwendungen
- die Entwicklung und Einführung neuer Druckkonzepte
- die Erneuerung von Programmplanungssystemen
- Recruiting-Anwendungen
- das Neue Nachrichtenhaus, einschließlich der Planung gemeinsamer Arbeitsplätze

Weiterhin wurden rund 85 Prüfungen von kleineren Softwareanwendungen, Apps und sonstigen digitalen Anwendungen angefragt.

b) Datensicherheit

Dieser Berichtspunkt soll aufgrund der Darstellung am Ende des Tätigkeitsberichts nicht den Eindruck erwecken, dass seine Bedeutung gering sei. Im Gegenteil: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt die Lage der IT-Sicherheit in Deutschland insgesamt als besorgniserregend ein. In seinem aktuellen Bericht kommt das BSI zu folgendem Ergebnis: „Die IT-Sicherheitslage in Deutschland insgesamt war im aktuellen Berichtszeitraum angespannt bis kritisch. Dies war zum einen auf die Ausweitung der bekannten cyberkriminellen Lösegelderpressungen hin zu ergänzenden Schweigegelderpressungen (sogenannte Double Extortion) und

Schutzgelderpressungen zurückzuführen. Zum anderen traten im aktuellen Berichtszeitraum jedoch auch Vorfälle auf, die eine Wirkung über die jeweils betroffenen Opfer hinaus entfalteten. Zudem haben Angreifer die Produktion neuer Schadsoftware-Varianten im Vergleich zum vorigen Berichtszeitraum deutlich beschleunigt. Wurden im vorigen Berichtszeitraum noch durchschnittlich 322.000 neue Varianten pro Tag bekannt, so lag der Tagesindikator im aktuellen Berichtszeitraum bei durchschnittlich 394.000 Varianten pro Tag. Das entsprach einem Zuwachs von gut 22 Prozent. Insgesamt haben Angreifer im aktuellen Berichtszeitraum damit rund 144 Millionen neue Schadprogramm-Varianten produziert."

Das Jahr 2021 war mithin gekennzeichnet durch erhebliche Gefahren der IT- und Datensicherheit. Für das BSI gilt daher: „Informationssicherheit muss einen deutlich höheren Stellenwert einnehmen und zur Grundlage aller Digitalisierungsprojekte werden." Die Probleme sind immens und global und nicht allein der Pandemie geschuldet. Zwar ergab eine Umfrage des Kriminologischen Forschungsinstituts Niedersachsen (KFN), dass sich grundsätzlich die pandemische Lage oftmals negativ auf die IT-Sicherheit von Unternehmen auswirkt hat. Geschuldet ist dies der vermehrten Tätigkeit im Homeoffice, jedenfalls wenn die Arbeit mit privater Hard- und Software verrichtet wird. Dem Forschungsbericht zufolge erhöhte dies das Risiko von Angriffen mit Schadsoftware und von Phishing-Attacken. Aber das grundlegende Problem sind weltweit durchgeführte Cyberattacken. Die digital vorgenommenen Angriffe haben durchaus das Potenzial, in die analoge Welt einzugreifen. So warnte der US-Präsident Joe Biden vor militärischen Auseinandersetzungen, deren Ursachen in Hackerattacken begründet sein können: „Ich denke, es ist mehr als wahrscheinlich, wenn wir in einem Krieg enden werden - einem echten Krieg mit einer Großmacht -, dass dieser die Folge eines Cyberangriffs von großer Tragweite wäre" (www.dw.com/de/biden-cyberangriffe-k%C3%B6nnten-zu-krieg-f%C3%BChren/a-58667836). Hintergrund dieser Äußerung dürften Cyberangriffe auf amerikanische Unternehmen gewesen sein (die Netzwerkmanagementfirma SolarWinds, die Colonial Pipeline, der Fleischverarbeitungsbetrieb JBS, die Softwarefirma Kaseya), die neben wirtschaftlichen Schäden auch die Kraftstoff- und Lebensmittelversorgung beeinträchtigten.

Aber auch der Blick nach Deutschland ist beunruhigend: In den Jahren 2020 und 2021 wurden nach einer Erhebung des Bitkom – befragt wurden 1067 Unternehmen – Schäden in Höhe von 223 Milliarden Euro verursacht. In den beiden Jahren zuvor waren es bereits 103 Milliarden Euro pro Jahr. 88 Prozent der befragten Unternehmen gaben an, bereits attackiert und erpresst worden zu sein (www.dw.com/de/220-milliarden-euro-schaden-durch-cyberangriffe/a-58767445). Viele Angriffe werden durch Ransomware verursacht. Dies ist Schadsoftware, die sich in vernetzten Systemen einnistet, Daten verschlüsselt und die zugriffsberechtigten Nutzer*innen erpresst. Durch die Zahlung eines Lösegelds werden die Daten (vielleicht) wieder freigegeben.

Derartige Angriffe verfolgen aber nicht immer wirtschaftliche, sondern oft auch politische Zwecke. Am Freitag, dem 9. Juli 2021, wurde erstmals in Deutschland ein digitaler Katastrophenfall ausgerufen worden. Der Landkreis Anhalt-Bitterfeld war am Rande der Handlungsunfähigkeit, zahlreiche administrative Vorgänge konnten nicht ausgeführt werden (z. B. die Auszahlung von Sozialhilfen). Die Gründe für die Attacken sind vielfältig, ebenso gilt dies für die Gruppen der Angreifer. Die Bedeutung entsprechender Angriffe geht daher über den Wirkungskreis eines Landkreises hinaus: „Die Bundesregierung hat sich in scharfem Ton gegen russische Beeinflussungsversuche vor der Bundestagswahl am 26. September verwahrt. Eine Sprecherin des Auswärtigen Amts forderte eine sofortige Einstellung der Cyber-Kampagnen und drohte der russischen Regierung mit Konsequenzen, sollte sie der Forderung nicht nachkommen. […] Der Bundesregierung liegen der Außenamtssprecherin zufolge ‚verlässliche Erkenntnisse' vor, demzufolge die Desinformationskampagne ‚Cyber-Akteuren des russischen Staates und konkret dem Militärgeheimdienst GRU zugerechnet werden können'" (www.dw.com/de/bundesregierung-fordert-von-russland-ende-der-cyberattacken/a-59100108). Immerhin hat die Bundesregierung reagiert und eine neue Strategie für Cybersicherheit beschlossen. Im Fokus der Strategie steht **der erhöhte Schutz von Behörden, sogenannter Kritischer Infrastruktur, Unternehmen und Bürger*innen vor Cyberattacken**. Dazu gehören soll eine frühzeitige Einbeziehung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in die Digitalisierungsvorhaben des Bundes. Auch soll

das BSI eine zentrale Rolle im Bund-Länder-Verhältnis erhalten und neben dem Bundeskriminalamt (BKA) und dem Bundesamt für Verfassungsschutz zu einer dritten Säule in einer föderal integrierten Cybersicherheitsarchitektur werden (www.dw.com/de/bundesregierung-mit-neuer-strategie-zur-hacker-abwehr/a-59123296).
Ende des Jahres musste das Bundesamt für Sicherheit in der Informationstechnik (BSI) sogar die **Warnstufe Rot** ausrufen, weil ein Teil einer Software namens Log4j eine schwerwiegende Sicherheitslücke darstellte. Log4j ist ein sogenanntes Open-Source-Werkzeug, das zur Protokollierung von Vorfällen in Java-Anwendungen benutzt wird. Die Schwachstelle (Log4shell) kann von Angreifern genutzt werden, um Server aus der Ferne zu übernehmen. Die Auswirkungen können sich noch Monate später entfalten. Das Thema Datensicherheit wird also dauerhaft aktuell bleiben.

Der NDR hatte ebenfalls mit Schwachstellen zu kämpfen, auch wenn es im Ergebnis glimpflich ausging. Zu tun hatte der NDR beispielsweise mit

- einem verdächtigen Verhalten, weil es bei einem System der Softwareverteilung mehrere vergebliche Anmeldeversuche und ungewöhnliche Meldungen gab, die auf einen Cyberangriff hindeuteten, womit eine forensische Untersuchung notwendig war,
- dem Umstand, dass im sogenannten Darknet eine Liste mit ca. 500 E-Mail-Adressen und Kennwörtern von NDR-Benutzer*innen veröffentlicht war (ohne dass es zu einem unbefugten Zugriff von außen gekommen ist),
- erpresserischen E-Mails,
- diversen Sicherheitslücken in Microsoft-Systemen, wie etwa der Schwachstelle „PrintNightmare“, einer Lücke im Windows Print Spooler Dienst, der in der Regel auf allen Windows Systemen läuft, mit der nach der Einschätzung des BSI eine weitgehende Kompromittierung mehrerer Systeme möglich ist.

Wegen der ständig wachsenden Bedrohungslage hatte der AKDSB seit rund zwei Jahren die Einführung eines Systems begleitet und vehement unterstützt und eingefordert, mit dem frühzeitig Angriffe erkannt und abgewehrt

werden können (ein sogenannter Pilotbetrieb war bereits eingerichtet worden). Diese Systeme zur Angriffserkennung (sog. Security Incident & Event Management Systeme, kurz „SIEM“) und -bewältigung sind einerseits nunmehr mit dem novellierten IT-Sicherheitsgesetz für bestimmte Branchen gesetzlich gefordert, andererseits auch tatsächlich wirksam um Schaden abzuhalten. **Um die endgültige Einführung nicht länger hinauszuzögern, war im Juli 2021 gemäß Art. 57 Abs. 1 lit. d) DSGVO eine Sensibilisierung derart auszusprechen, dass unverzüglich geeignete technische und organisatorische Maßnahmen zu ergreifen sind, um die Sicherheit von personenbezogenen Daten zu gewährleisten**. Dazu zählt der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Ein SIEM/SOC ist eine solche technische und organisatorische Maßnahme, für deren unverzügliche Etablierung vom Verfasser dieses Berichts eingetreten wurde. Denn die Einführung entsprechender Erkennungssysteme ist datenschutzrechtlich geboten und erforderlich (Art. 5, 25 DSGVO). Bei der Wahl des Modells eines Systems zur Angriffserkennung und -abwehr (Fremd- oder Mischbetrieb) war überdies zu beachten, dass ein komplettes Outsourcing sowohl des SIEM (Protokollierungssystem), als auch des SOC (die Auswertung der Protokolle) datenschutzrechtlich nicht vorzugswürdig ist. Die interne Lösung für das SIEM und ein Outsourcing für das SOC hingegen ist unbedenklich, weil damit die Datenhaltung der sensiblen Logging-Daten bei den verantwortlichen Rundfunkanstalten verbleibt.

Neben solchen System haben der NDR und der Rundfunkdatenschutzbeauftragte weitere Maßnahmen erörtert und ergriffen, um die Eintrittswahrscheinlichkeit von Schäden und Ausfällen aufgrund des Einsatzes von Technologien zu minimieren. Dazu gehörte auch der von der Datenschutzgrundverordnung geforderte und stärker bei der Anschaffung in den Fokus genommene Grundsatz des „Security by Design“, also der Beachtung sicherheitsrelevanter Anforderungen von Beginn an. Weiterhin gilt es, sogenannte Awareness Maßnahmen zu stärken, also den Beschäftigten vermehrt das notwendige Bewusstsein für Sicherheitsbelange zu vermitteln.

F. Anfragen nach dem Informationszugang

Wie eingangs unter B. erwähnt, sind die Aufgaben des Rundfunkdatenschutzbeauftragten seit September 2021 erweitert worden. Mit der Einführung des Informationsfreiheitsanspruches gegen den NDR (§ 47 NDR Staatsvertrag) können Antragstellende, die der Ansicht sind, dass ein Informationsanspruch zu Unrecht abgelehnt, nicht beachtet oder nur unzulänglich beantwortet ist, sich an den Rundfunkdatenschutzbeauftragten wenden. Diesbezüglich wurde bis Ende Dezember 2021 nur eine Zuschrift eingereicht in der moniert wurde, dass eine Anfrage nicht binnen der Monatsfrist (§ 47 NDR Abs. 5 Staatsvertrag) nach Eingang beantwortet worden sei. Dies war zutreffend. Immerhin hat der NDR hat zeitnah reagiert, eine Entschuldigung ausgesprochen und die Anfrage beantwortet.

Eine weitere Anfrage betraf nicht den NDR, sondern die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR bezüglich der Anzahl und des Umgangs mit Beschwerden zu einer bestimmten Thematik. Die kurz vor Jahresende eingereichte Anfrage konnte im Berichtszeitraum nicht mehr bearbeitet werden.

G. Fazit und Ausblick

Datenschutzrechtliche Belange spiegeln den gesamten Geschäftsbetrieb wider. Die Spannbreite reicht von der Betroffenheit einzelner Personen bis hin zu übergreifenden Geschäftsprozessen und Infrastrukturanwendungen. Als zentrales Grundrecht einer digitalisierten Gesellschaft ist der Schutz der informationellen Selbstbestimmung aus dem Alltag nicht mehr wegzudenken.

Es finden derzeit, wie eingangs erwähnt, grundlegende Änderungsprozesse statt: Personenbezogene Daten werden immer weniger auf eigenen Servern und in eigenen Räumlichkeiten (On-Premise), sondern vermehrt durch Anbieter von Cloud-Diensten verarbeitet. Die datenschutzrechtlichen Risiken steigen dadurch und der Befassungsaufwand verlagert sich. Denn die eigene Kontrolle über Systeme weicht immer mehr vertraglichen Konstruktionen mit Dritten, weil die Infrastruktur nicht mehr in den eigenen Händen gehalten wird. Insoweit bleibt zu hoffen, dass tatsächlich der „sichere Hafen für Europas Daten“ – Gaia-X als europäisches Datenökosystem – zeitnah zur Verfügung steht (https://www.dw.com/de/gaia-x-ein-sicherer-hafen-f%C3%BCr-europas-daten/a-59629149).

Da die Möglichkeiten lokaler Speicherungen und individueller Konfigurationen weniger werden, bedarf es zudem stärkerer Sicherungsmaßnahmen und Administrationsaufwänden, um ein hinreichendes datenschutzrechtliches Niveau zu erreichen. Zudem steigen die Abhängigkeiten zum Diensteanbieter und zum Internet. Es hat sich daher ein „Hybrid-Betrieb“, also eine Mischung aus On-Premise und Cloud-Nutzungen, herausgebildet. Ob dies mittel- und langfristig so bleiben wird, bleibt abzuwarten. Die Architektur der Infrastruktur wird sich angesichts der Dynamik von digitalisierten Geschäftsprozessen sicherlich noch öfter wandeln. Der Wunsch nach, aber auch das verfassungsrechtlich garantierte Recht auf (digitale) Selbstbestimmung wird hingegen unverändert bestehen bleiben und durchgesetzt werden müssen.