NORDDEUTSCHER RUNDFUNK

Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten des NDR

für das Berichtsjahr 2023

Dr. Heiko Neuhoff

Hamburg im Januar 2024

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 2023.

Danksagung

Meiner Mitarbeiterin sei für die Unterstützung des Rundfunkdatenschutzbeauftragten des NDR in allen Angelegenheiten und bei der Erstellung dieses Berichts herzlich gedankt.

Inhalt

A. Einleitung

Im Bemühen um eine kompakte, klare und gut verständliche Darstellung der Tätigkeiten der datenschutzrechtlichen Aufsichtsbehörde des NDR wurde der Bericht für das Jahr 2023 erstellt, obgleich das Jahr geprägt war von herausfordernden Aufgaben und revolutionären Entwicklungen. Wissenschaftler haben Nachweise gefunden, dass die Erde nun in einem neuen Zeitalter angekommen ist. Die Erde ist nun im „**Zeitalter des Menschen**" – Anthropozän – genannt, angekommen. Dieses neue geologische Zeitalter ist gekennzeichnet durch menschliches Handeln, weil der Mensch nachweisbar in die biologischen, geologischen und atmosphärischen Prozesse auf der Erde eingreift. Der Mensch prägt mithin belegbar das neue Erdzeitalter über die Umwelt, besser gesagt durch Schädigungen der Umwelt.

Während der Mensch also nun die Umwelt maßgeblich prägt, übergibt er zugleich bislang noch nicht absehbare Bereiche menschlichen Handels an Techniken: **Anwendungen der Künstlichen Intelligenz (KI)** sind beispielsweise in der Lage, Texte (z. B. journalistischer oder wissenschaftlicher Art), Software-Codes, Bilder und Videos zu erstellen oder menschliche Stimmen zu erzeugen und Musikstücke zu komponieren. Dass der Einsatz von Anwendungen der KI auch eine datenschutzrechtliche Herausforderung darstellt, dürfte selbsterklärend sein. Sogar ein Entwickler und Anbieter von KI (OpenAI) warnt wie folgt vor den Gefahren:

„Superintelligenz wird die einflussreichste Technologie sein, die die Menschheit je erfunden hat und könnte uns helfen, viele der wichtigsten Probleme der Welt zu lösen. Aber die enorme Macht der Superintelligenz könnte auch sehr gefährlich sein und zur Entmachtung der Menschheit oder sogar zum Aussterben der Menschheit führen. […] Derzeit haben wir keine Lösung, um eine potenziell superintelligente KI zu steuern oder zu kontrollieren und zu verhindern, dass sie abtrünnig wird. Unsere aktuellen Techniken zur Ausrichtung der KI, wie beispielsweise das verstärkende Lernen aus menschlichem Feedback, basieren auf der Fähigkeit des Menschen, die KI zu überwachen. Aber Menschen werden nicht in der Lage sein, KI-Systeme zuverlässig zu überwachen, die viel intelligenter sind als wir. Daher lassen sich unsere derzeitigen Ausrichtungstechniken nicht auf Superintelligenz übertragen. Wir brauchen neue wissenschaftliche und technische Durchbrüche" (https://openai.com/blog/introducing-superalignment#fn-A – abgerufen am 14.11.2023).

Eine Vielzahl von möglichen Gefahren durch den Einsatz von KI (etwa Kriegsführungen, Entwicklung neuer Waffen, Kontroll- und Sicherheitsverluste, Zunahme und mangelnde Verifizierbarkeit von Falschinformationen) haben KI-Experten vom Center for AI Safety (Zentrum für KI-Sicherheit) in einer Stellungnahme zusammengefasst (https://www.safe.ai/ai-risk). Danach könnte der Mensch vollständig von Maschinen abhängig werden, ohne diese wirksam kontrollieren zu können.

Der Mensch hat die Erde mithin seinem Handeln unterworfen und geologisch das „Zeitalter des Menschen" eingeläutet. Gleichzeit unterwirft er sich nun selbst der Künstlichen (maschinellen) Intelligenz. Gesellschaftlich dürfte mithin das „**Zeitalter der Maschinen**" entstanden sein. Beide Prozesse erscheinen derzeit noch weitgehend ungesteuert. Daher **erfordert KI auch verstärktes datenschutzrechtliches Handeln**, um zumindest das Recht auf informationelle Selbstbestimmung zu garantieren. **Zum diesbezüglichen Stand im NDR wird unter E. II. 5. B) eingegangen**.

B. Rechtsgrundlagen und Zuständigkeiten des Rundfunkdatenschutzbeauftragten des NDR

Die §§ 43 bis 46 NDR Staatsvertrag und die Datenschutzgrundverordnung (DSGVO) sind die maßgeblichen Rechtsgrundlagen für den Auftrag und die Aufgaben des Rundfunkdatenschutzbeauftragten des NDR. Als Aufsichtsbehörde nach Art. 51 DSGVO obliegt ihm die Überwachung der Einhaltung der Datenschutzvorschriften bei der **gesamten Tätigkeit des NDR und seiner Beteiligungsunternehmen** im Sinne der §§ 40 ff. Medienstaatsvertrag.

Die Prüfung von Beschwerden nach § 47 NDR Staatsvertrag gehört ebenso dazu. Sofern ein Informationsanspruch nach Ansicht einer antragstellenden Person zu Unrecht abgelehnt, nicht beachtet oder nur eine unzulängliche Antwort gegeben worden ist, kann der Rundfunkdatenschutzbeauftragte zwecks Prüfung der Angelegenheit angerufen werden.

C. Personalien

In der seit dem 25. Mai 2022 andauernden zweiten Amtszeit des Rundfunkdatenschutzbeauftragten des NDR hat es keine personelle Änderungen gegeben. Der Verfasser dieses Berichts ist außerdem der stellvertretende Vorsitzende der Rundfunkdatenschutzkonferenz und für den Fall einer Verhinderung des Rundfunkbeauftragten für den Datenschutz des

MDR über einen Zeitraum von länger als 2 Monaten sein Stellvertreter (Art. 2 Abs. 3 der Satzung über die Rundfunkbeauftragte für den Datenschutz des MDR).

D. Wesentliche Entwicklungen im Berichtszeitraum

Die Vielzahl der Entwicklungen mit datenschutzrechtlicher Relevanz für den öffentlich-rechtlichen Rundfunk und seine Beteiligungsunternehmen erfordert in diesem Bericht eine Reduktion auf wesentliche Aspekte. Während im Tätigkeitsbericht für das Jahr 2022 an dieser Stelle eine auch historische Übersicht über Regelungen dargestellt wurde, die der Wahrung von Geheimnissen und dem Schutz höchstpersönlicher Angelegenheiten dienen sollten, wird hier in die Gegenwart und (hoffentlich) nahe Zukunft geblickt.

I. EU-Kommission

Datenverarbeitungen erfolgen in einer Vielzahl von Fällen über Ländergrenzen hinweg. Europäische und internationale Regelungen sind daher von großer Bedeutung.

1. Richtlinie über KI-Haftung und KI-Verordnung

Die ebenso populären wie mächtigen Anwendungen der KI sollen nach dem Willen der EU-Kommission reguliert werden. Mit dem „**Entwurf für eine Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz**“ sollen Haftungslücken geschlossen werden, die durch den Einsatz von KI entstanden sind. Unternehmen sollen etwaige Haftungsrisiken besser einschätzen können. Zugleich soll durch die Risikominimierung und Rechtsklarheit die Einführung, Verbreitung und Weiterentwicklung von KI-Systemen in der Europäischen Union gefördert werden.

Anfang Dezember 2023 haben sich Unterhändler des EU-Parlaments, des Ministerrats und der Kommission in Brüssel auf eine KI-Verordnung verständigt. Die Verordnung soll in den kommenden Monaten in Kraft treten und erstmals verbindliche Vorgaben für den Einsatz von KI schaffen („**Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz**“). Ziel der Verordnung ist, KI grundsätzlich zu regeln. Angedacht ist eine Klassifikation von Anwendungen der KI nach Risiken (risikoarme, begrenzt riskante, verbotene KI). Verboten wäre danach

etwa eine KI, die biometrische Kategorisierungen anhand sensitiver Eigenschaften vornimmt (nach politischen oder religiöse Überzeugungen oder der sexuelle Orientierung). Gleiches gilt auch für sogenannte Social-Scoring-Systeme, die das Verhalten von Menschen bewerten, und eine automatisierte Erkennung von Emotionen. Ausnahmen sollen allerdings für Strafverfolgungsbehörden gelten. Das Regelungsziel ist:

„Durch ihre besonderen Merkmale (z. B. Undurchsichtigkeit, Komplexität, Datenabhängigkeit, autonomes Verhalten) kann die Verwendung von KI dazu führen, dass einige der in der EU-Grundrechtecharta (im Folgenden die „Charta“) verankerten Grundrechte verletzt werden. Der Vorschlag zielt darauf ab, diese Grundrechte in hohem Maße zu schützen und durch einen klar festgelegten risikobasierten Ansatz verschiedene Ursachen für Risiken anzugehen“ (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206).“ Mit anderen Worten soll also auch das Recht auf informationelle Selbstbestimmung geschützt werden.

Es handelt sich noch um Entwürfe, so dass geltende und wirksame Regulierungen abzuwarten bleiben. Denn gerade mit der KI-Verordnung kann ein wesentlicher Beitrag zum Schutz des Datenschutzrechts/des Rechtes auf informationelle Selbstbestimmung geleistet werden. Zudem braucht es Antworten auf die Fragen,

- wo ethische Grenzen für den Einsatz von KI gezogen werden,
- wie eine Kontrollierbarkeit von KI gewährleistet werden kann und
- in welcher Weise demokratische Freiheiten und Grundrechte garantiert werden.

2. Trans-Atlantic Data Privacy Framework (DPF)

Am 10. Juli 2023 hat die EU-Kommission den **Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union und den USA** angenommen. Das Trans-Atlantic Data Privacy Framework (DPF) hält fest, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen des DPF aus der EU an US-Unternehmen übermittelt werden. „Angemessen“ meint, dass die USA ein mit dem der Europäischen Union vergleichbares Datenschutzniveau vorweisen können.

Der Europäische Gerichtshof (EuGH) hat bereits zwei Abkommen vor dem DPF (Safe Harbour, EuGH, 06.10.2015 – C-362/14 “Schrems I”; Privacy Shield, EuGH, 16.07.2020 – C-311/18 “Schrems II”) für unwirksam erklärt. Mit dem neuen Abkommen soll den Bedenken des Gerichts Rechnung getragen werden, indem neue verbindliche Garantien eingeführt werden, etwa die Beschränkung des Zugriffs auf EU-Daten durch US-Geheimdienste auf ein notwendiges und verhältnismäßiges Niveau. Zudem haben die USA ein Datenschutzüberprüfungsgericht errichtet (Data Protection Review Court, DPRC), zu dem EU-Bürger*innen Zugang haben sollen.

Das DPF ist mithin das dritte Regelwerk für eine rechtskonforme Datenübermittlung in die USA. Bis zum Inkrafttreten des DPF am 10. Juli 2023 waren Unternehmen gehalten, andere Maßnahmen für einen Datentransfer zu ergreifen. Zumindest waren Standardvertragsklauseln („SCC“) abzuschließen, um den Schutz von personenbezogenen Daten in einem sogenannten „unsicheren Drittstaat“ sicherzustellen. Daneben waren weitere technische Maßnahmen erforderlich. Der Europäische Datenschutzausschuss (EDSA) sah beispielsweise Verschlüsselungen oder Anonymisierungen von personenbezogenen Daten vor einem Transfer für geboten an.

Das DPF soll Rechtssicherheit schaffen und Restrisiken durch folgende Neuerungen zumindest minimieren:

Die USA haben ein zweistufiges Rechtsbehelfsverfahren etabliert, in dem über Beschwerden von betroffenen Personen, deren Daten aus dem EWR an Unternehmen in den USA übermittelt wurden, geprüft werden sollen. In einem Beschwerdeverfahren können EU-Bürger*innen eine Beschwerde beim “Civil Liberties Protection Officer” erheben. Die Beschwerde kann bei einer europäischen Datenschutzbehörde eingereicht werden. Diese gibt die Eingabe an den Officer (einem Bürgerrechtsbeauftragten der US-Nachrichtendienste) zur Prüfung weiter. In einer zweiten Stufe kann in einem Überprüfungsverfahren die Entscheidung des Officers angefochten werden. Der „Data Protection Review Court” entscheidet über die Beschwerde und kann etwa die Löschung von Daten anordnen, wenn gegen Schutzmaßnahmen verstoßen wurde. Weiterhin haben sich die USA verpflichtet, den Zugriff auf Daten von EU-Bürger*innen auf das zum Schutz der nationalen Sicherheit erforderliche und verhältnismäßige Maß zu beschränken.

Ob – und gegebenenfalls wie lange – das Abkommen Bestand haben wird, bleibt abzuwarten. Erste Klagen wurden bereits angekündigt.

3. Bußgeldzumessungen

Nicht die EU-Kommission, sondern der insoweit zuständige Europäische Datenschutzausschuss (EDSA) hat in seiner Sitzung vom 24. Mai 2023 die **endgültigen Leitlinien zur Bußgeldzumessung** nach einer öffentlichen Konsultation angenommen. Damit folgt nun die Verhängung von Bußgeldern einem im Geltungsbereich der DSGVO einheitlichen Konzept. Verstöße gegen datenschutzrechtliche Bestimmungen können teuer sein. So hat etwa die irische Datenschutzaufsichtsbehörde aufgrund angenommener Datenschutzverstöße bei Facebook gegen den Konzern Meta ein Bußgeld in Höhe von 1,2 Milliarden Euro verhängt. Meta soll unzulässigerweise personenbezogene Daten in die USA übermittelt haben. Rechtsmittel gegen den Bescheid wurden angekündigt. Eine Überprüfung der rund 200 Seiten langen Entscheidung bis hin zu einem rechtskräftigen Urteil dürfte einige Jahre in Anspruch nehmen.

II. Rechtsprechung

Die Rechtsprechung war sehr aktiv. Eine Reihe von Entscheidungen mit datenschutzrechtlichem Bezug sind ergangen. Die folgenden Punkte sind nur ein kleiner Ausschnitt wesentlicher Prozesse und Entscheidungen.

1. Facebook-Fanpages

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hatte mit einem Bescheid vom 17.02.2022 die Verarbeitung von personenbezogenen Daten über die Facebook-Fanpage des Bundespresseamtes (BPA) untersagt. Zur Begründung wurde angeführt, dass ein datenschutzkonformer Betrieb einer solchen Seite nicht möglich sei. Hintergrund ist eine Entscheidung des EuGH vom 5. Juni 2018 (Rechtssache C-210/16), in der das Gericht festgestellt hatte, dass eine datenschutzrechtliche Mitverantwortung für Betreiber einer Facebook-Fanpage bestehe.

Das BPA hat nun Klage gegen die Untersagung erhoben. Das Verfahren vor dem Verwaltungsgericht Köln dauert noch an. Aus Sicht des BPA ist der Betrieb einer solchen

Seite notwendig und das Informationsinteresse höher zu bewerten als etwaige datenschutzrechtliche Verstöße:

„Die Bundesregierung hat einen verfassungsrechtlichen Auftrag, die Bürgerinnen und Bürger über die Tätigkeit, Vorhaben und Ziele der Bundesregierung zu informieren. Zur Erfüllung dieses Auftrags gehört es, sich an der tatsächlichen Mediennutzung der Bürgerinnen und Bürger zu orientieren, um diese auch wirklich zu erreichen. […] Es geht in diesem Verfahren um die Klärung grundsätzlicher, komplexer Sach- und Rechtsfragen zum europäischen Datenschutzrecht. Diese können im Ergebnis jeden Betreiber einer Facebook-Seite in der EU betreffen: nicht nur staatliche Institutionen auf allen Ebenen, sondern auch Parteien oder private Stellen. […] Auf sozialen Medien aktiv zu sein, bedeutet im Übrigen nicht, sich mit allen Einzelheiten der Geschäfts- und Datenschutzpraxis der jeweiligen Unternehmen einverstanden zu erklären“ (https://dip.bundestag.de/vorgang/beibehaltung-der-social-media-kan%C3%A4le-der-bundesregierung-entgegen-des-rates-des-bundesdatenschutzbeauftragten/297394).

Wann eine Entscheidung ergeht und welche Konsequenzen gegebenenfalls auch für den öffentlich-rechtlichen Rundfunk daraus zu ziehen sind, ist noch nicht abzusehen.

2. Schadensersatz für Datenschutzverstöße

Die Frage, unter welchen Voraussetzungen Schadensersatz für Verstöße gegen datenschutzrechtliche Bestimmungen anzuerkennen ist, hatte die nationalen Gerichte schon seit geraumer Zeit beschäftigt. Der EuGH hat nun festgestellt, dass ein bloßer Verstoß gegen die Vorschriften der DSGVO nicht ausreicht, um einen Anspruch auf Schadensersatz zu begründen (EuGH, Urteil vom 04.05.2023, Rs. C-300/21). Voraussetzung für den Anspruch in Art. 82 Abs. 1 DSGVO geregelten Anspruch ist vielmehr, dass

- ein Verstoß gegen die DSGVO vorliegt,
- aus diesem Verstoß ein materieller oder ein immaterieller Schaden entstanden ist und
- dieser Verstoß tatsächlich kausal für den Schaden ist.

Weiterhin muss eine gewisse Erheblichkeitsschwelle erreicht sein. Die Einzelheiten sind nationalen Regelungen zu entnehmen.

3. Zum Recht auf Auskunft über die Verarbeitung personenbezogener Daten

Zahlreiche Entscheidungen zum Umfang und zur Form des Auskunftsanspruches nach Art. 15 DSGVO sind ergangen.

Mit Urteil vom 26. Oktober 2023 (Rs. C-307/22) entschied der EuGH, dass derartige Auskünfte **grundsätzlich unentgeltlich** zu erteilen sind. Ein Entgelt kann nur dann verlangt werden, wenn bereits eine (inhaltsgleiche) Auskunft erteilt wurde.

Weiterhin kann, so der EuGH (Urteil vom 22.06.2023, Rs. C-579/21), das Auskunftsrecht nach Art. 15 DSGVO auch Informationen darüber beinhalten, wann und warum personenbezogenen Daten des Betroffenen verarbeitet wurden.

Jedenfalls darf die Geltendmachung des Anspruches aber **nicht rechtsmissbräuchlich** sein. Einen solchen Fall hatte das OLG Karlsruhe angenommen (Urteil vom 29.11.2022, Az. 12 U 305/21), weil der zu beurteilende Anspruch offenkundig weder eine datenschutzrechtliche noch anderweitige legitime Zielsetzung verfolgte. Das Landesarbeitsgericht Berlin hat diesbezüglich eine großzügigere Auffassung (Urteil vom 30.03.2023, Az. 5 Sa 1046/22). Danach könnten Ansprüche auf Auskunft auch dann noch auf Art. 15 DSGVO gestützt werden, wenn sie nicht ausschließlich oder ganz überwiegend aus datenschutzrechtlichen Erwägungen geltend gemacht werden. Mit den Grenzen des Auskunftsersuchen hat sich auch das OLG Düsseldorf befasst (Beschluss vom 13.07.2023, Az. I-13 U 102/22, I-13 U 44/23). Danach ist ein Antrag auf Auskunft rechtsmissbräuchlich, wenn die antragstellende Person sich „[…] Informationen beschaffen [möchte], die ihm bereits in verständlicher Form vollständig vorliegen […]“. Da im zu beurteilenden Fall keine Ausnahme vorliege, in der die erneute Auskunft zur Prüfung der Rechtmäßigkeit der Datenverarbeitung erforderlich sei, sei auch kein berechtigtes Interesse an der Auskunft gegeben. Der Betroffene wolle vielmehr versuchen, sich durch das Auskunftsersuchen „[…] aus Bequemlichkeit und unter Umgehung zivilprozessualer Grundsätze seiner Beibringungspflicht zu entledigen […]“. Dies sei eine Zweckentfremdung des Anspruchs.

4. Beschäftigtendatenschutz

Das Landesarbeitsgericht Baden-Württemberg hatte einen Fall zu beurteilen, in dem der Arbeitgeber den **E-Mail-Account eines Mitarbeiters** ausgewertet hatte (Urteil vom 27.01.2023, Az. 12 Sa 56/21). Da private Nachrichten gefunden wurden, folgte eine Kündigung. Im Kündigungsschutzprozess machte der Mitarbeiter mit Erfolg geltend, dass es kein ausdrückliches Verbot einer privaten Nutzung gegeben habe. Die sowohl private als auch dienstliche Nutzung der technischen Infrastruktur und der bereitgestellten Endgeräte sei erlaubt gewesen. Das LAG Baden-Württemberg gab dem Kläger Recht und verurteilte den Arbeitgeber wegen Datenschutzverstößen zur Zahlung eines Schmerzensgeldes. Zudem unterlägen die ausgewerteten E-Mails einem Beweisverwertungsverbot. Die Kündigung war somit unwirksam (zur Situation im NDR s. unter E. II. 4. g)).

Der Europäische Gerichtshof hat sich mit dem Hessischen Datenschutzgesetz befasst und mit Urteil vom 30. März 2023 (Rs. C-34/21) entschieden, dass die dortige Vorschrift zum Beschäftigtendatenschutz (§ 23 HDSIG) nicht mit der DSGVO vereinbar ist. Die Entscheidung ist auch außerhalb Hessens insoweit von Bedeutung, als die Vorschrift fast wortgleich mit der entsprechenden Regelung im Bundesdatenschutzgesetz ist (§ 26 BDSG). Der EuGH hat festgestellt, dass die Verarbeitung personenbezogener Daten von Lehrkräften beim Livestreaming von Schulunterricht („Homeschooling“) in den Anwendungsbereich der DSGVO fällt. Die Regelung des § 23 HDSIG genüge aber nicht den Anforderungen an eine „spezifischere“ Vorschrift (Art. 88 Abs. 2 DSGVO), um die erforderliche Öffnungsklausel zur Datenverarbeitung im Beschäftigungskontext auszufüllen.

Insgesamt ist aus der Entscheidung abzuleiten, dass der **nationale Gesetzgeber bezüglich des Beschäftigtendatenschutzes detailliertere Regelungen** erlassen muss, auch wenn in Beschäftigungsverhältnissen auf die Regelungen der DSGVO zurückgegriffen werden kann.

Ob und wie der (Bundes-) Gesetzgeber auf diese Entscheidung reagiert, bleibt abzuwarten. Jedenfalls existiert ein Referentenentwurf zur Novellierung des BDSG. Ob dort oder in einem eigenen Beschäftigtendatenschutzgesetz Regelungen erlassen werden, ist noch offen. Die Forderungen nach einem eigenständigen Beschäftigtenda-

tenschutzgesetz bestehen schon lange und auch der aktuelle Koalitionsvertrag hat dies zum Inhalt.

E. Tätigkeiten des Rundfunkdatenschutzbeauftragten des NDR im Jahr 2023

Die Erfüllung der Aufgaben erfordert eine Zusammenarbeit und Vernetzung mit anderen Aufsichtsbehörden und Datenschutzbeauftragten. Dies stellt sich wie folgt dar.

I. Zusammenarbeit und Vernetzung

Folgende Gremien und Kreise sind von besonderer Relevanz:

- Die **Rundfunkdatenschutzkonferenz** (RDSK): Das sind die als datenschutzrechtliche 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, ARTE und der Schweizerischen Radio- und Fernsehgesellschaft.
- Die **Datenschutzkonferenz** (DSK): Das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder.

Informationsangebote der Rundfunkdatenschutzkonferenz, der Datenschutzkonferenz und des Virtuellen Datenschutzbüros (ein gemeinsames Angebot von Datenschutzinstitutionen unter der Verantwortung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein) sind hier zu finden:

https://www.rundfunkdatenschutzkonferenz.de/
https://www.datenschutz.de/
https://www.bfdi.bund.de/DE/Home/home_node.html
https://www.datenschutzkonferenz-online.de/

1. Die Rundfunkdatenschutzkonferenz (RDSK)

Die Aufgaben der RDSK leiten sich neben den gesetzlichen Vorgaben insbesondere aus der Notwendigkeit gemeinsamen Handels ab, da die Rundfunkanstalten Koope-

rationen eingegangen sind und gemeinsame Einrichtungen unterhalten. Es besteht daher ein **Erfordernis, einheitliche datenschutzrechtliche Standards zu definieren**, zu gleichlautenden Auslegungen datenschutzrechtlicher Vorschriften zu kommen und abgestimmte Orientierungshilfen, Handreichungen und Positionspapiere zu erarbeiten. Die RDSK tauscht sich bei Bedarf aus und tagt mindestens zwei Mal im Kalenderjahr. Die Grundlagen der Zusammenarbeit sind einer Geschäftsordnung zu entnehmen:

https://www.rundfunkdatenschutzkonferenz.de/ueber-uns.

Nicht nur der föderale Medienverbund der ARD, sondern auch das ZDF, das Deutschlandradio und die Tochterunternehmen, Einrichtungen und Beteiligungen der Sendeanstalten fallen unter die Aufsicht der Rundfunkdatenschutzbeauftragten. Der **allgemeine Geschäftsbetrieb** der Rundfunkanstalten, die datenschutzrechtlichen **Herausforderungen der Digitalisierung** und nun auch die noch nicht absehbaren Folgen aus dem **Einsatz von KI** sind von der RDSK zu überwachen, die datenschutzrechtlichen Vorgaben durchzusetzen und die weiteren Aufgaben aus dem Katalog des Art. 57 DSGVO zu erfüllen.

Die bereits im letzten Tätigkeitsbericht vorgebrachten Bedenken gegen eine Verringerung der Mitgliederzahl der RDSK sollen hier nicht wiederholt werden, auch wenn die Einwände noch immer aktuell sind: Die Anforderungen sind gestiegen,

- etwa durch fortschreitende Regulierungen,
- umzusetzende Gerichtsentscheidungen,
- teilweise weitere Aufgaben hinsichtlich der Informationsfreiheit und
- dem technischen Fortschritt,

hingegen hat sich die **Anzahl der Mitglieder der RDSK seit ihrer Gründung halbiert**. Die Entwicklung ist bedenklich, weil der notwendige Austausch beschnitten wird und Möglichkeiten der Arbeitsteilung untereinander und Vernetzungen mit anderen Behörden abnehmen.

a) Organisation der RDSK

Die „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten“ und die „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten“ bilden die Grundlagen für die Arbeitsverteilung. Aufgrund der genannten personellen Veränderungen in der RDSK und tatsächlichen Entwicklungen in den Anstalten waren Anpassungen erforderlich. Noch immer gilt grundsätzlich das Prinzip der Verteilung der Aufsichten gemäß dem Sitz der beaufsichtigten Einrichtung, sofern gesetzliche Gründe nicht dagegen sprechen.

b) Tätigkeitsschwerpunkte der RDSK

Die RDSK hat u. a. beraten über die zukünftige Zusammenarbeit mit der DSK, koordinierte **Prüfungen der Nutzungsmessung** in den Telemedienangeboten der Rundfunkanstalten, Einzelfälle der **Auswirkungen des Medienprivilegs**, Anforderungen an **Datenschutzfolgeabschätzungen** und dem Erfordernis der Erstellung eines **Bußgeldkatalogs**.

Wie bereits oben unter D. I. 3. erwähnt, hat der Europäische Datenschutzausschuss (EDSA) **Leitlinien zur Bußgeldzumessung** angenommen, so dass Bußgelder im Geltungsbereich der DSGVO nach einem einheitlichen Konzept verhängt werden können. Aufgrund der europaweiten Harmonisierung werden auch die Aufsichtsbehörden über den öffentlich-rechtlichen Rundfunk die Leitlinien zur Bußgeldzumessung anwenden.

Ebenso wie die staatlichen Datenschutzaufsichtsbehörden mit Blick auf staatliche Stellen, haben die Datenschutzaufsichten über den öffentlichen Rundfunk keine Befugnis, Geldbußen im Sinne des Art. 58 Abs. 2 lit. i) DSGVO gegen Rundfunkanstalten zu verhängen. So sieht § 24 Abs. 3 des Hamburgischen Datenschutzgesetzes beispielsweise vor, dass der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit grundsätzlich keine Befugnis hat, gegenüber Behörden und öffentliche Einrichtungen Geldbußen zu verhängen. Vergleichbare Regelungen hat der Gesetzgeber auch für die Rundfunkdaten-

schutzbeauftragten geschaffen. So kann beispielsweise der Rundfunkdatenschutzbeauftragte des NDR **gegenüber dem NDR keine Geldbußen verhängen** (§ 46 Abs. 1 S. 4 NDR Staatvertrag). Die Aufsichtsbefugnisse der Datenschutzaufsichten nach Art. 58 DSGVO sind jedoch dann nicht beschränkt, wenn es sich um **Tochterunternehmen** der Rundfunkanstalten handelt. Im Rahmen des § 40 Medienstaatsvertrag ist es den Rundfunkanstalten gestattet, kommerzielle Tätigkeiten auszuüben. Diese Tätigkeiten dürfen nur unter Marktbedingungen erbracht werden und sind durch rechtlich selbständige Tochtergesellschaften zu erbringen. Aufgrund der Marktteilnahme der Tochtergesellschaften kommt im Falle eines Verstoßes gegen datenschutzrechtliche Vorgaben auch die Aufsichtsmaßnahme des Art. 58 Abs. 2 lit i) DSGVO – mithin die Verhängung einer Geldbuße – in Betracht.

Außerdem wurden aufgrund entsprechender Anlässe

- eine **Empfehlung zum Data Privacy Framework**,
- eine Orientierungshilfe zum **datenschutzkonformen Einsatz von KI** im öffentlich-rechtlichen Rundfunk und
- eine Handreichung zu **Mastodon**

erstellt:

Das **Data Privacy Framework** (DPF) erleichtert zwar einen Datentransfer in die USA (s. o. D. I. 2). Gleichwohl war zu empfehlen, entsprechende Datenübermittlungen besonders abzusichern, denn das Abkommen entfaltet seine Wirkung nur dann, wenn der Datenimporteur, also das Unternehmen, an das personenbezogene Daten übermittelt werden, auch unter dem DPF zertifiziert ist. **Zertifizierungen sind mithin zu prüfen und weitere Schutzmaßnahmen** zu ergreifen, weil:

Ein Jahr nach dem Inkrafttreten des DPF, und dann auch regelmäßig, soll von der Europäischen Kommission und den Vertretern der europäischen Datenschutzbehörden (EDSA) gemeinsam mit den zuständigen US-Behörden geprüft werden, ob die Vereinbarungen umgesetzt wurden und der neue Rechtsrahmen tatsächlich funktioniert. Ob das DPF langfristig Rechtssicherheit schafft,

bleibt mithin abzuwarten. Der EuGH könnte gegebenenfalls erneut einen Angemessenheitsbeschluss mit sofortiger Wirkung für ungültig erklären. Verantwortliche müssten dann umgehend reagieren. Daher hat die RDSK empfohlen, weiterhin **technische Maßnahmen einzusetzen**, um den Schutz personenbezogener Daten zu gewährleisten. Daneben wurde an **weitere Erfordernisse** und Prüfungen erinnert. Das entsprechende Papier und weitere Veröffentlichungen sind hier abrufbar:
https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen

Zum **Umgang mit KI** wird unter E. II. 5. b) ausgeführt.

Da einige Anstalten im Laufe des Jahres einen weiteren Verbreitungsweg beschritten hatten, namentlich das **Netzwerk Mastodon**, hat die RDSK ein entsprechendes Papier zur Funktionsweise und dortigen Verarbeitung von personenbezogenen Daten erstellt.

Weitere Themen waren Überlegungen zu einem Leitfaden für die datenschutzgerechte Gestaltung von **Telemedienangeboten für Kinder**, eine Verständigung zu **Einwilligungs- bzw. Cookie-Bannern** und die Evaluation der aktuellen Rechtsprechung.

c) Degeto

Bei den obigen Ausführungen zur Organisation der RDSK wurde erwähnt, dass die Aufsicht grundsätzlich nach dem Prinzip des Sitzes der beaufsichtigten Einrichtung verteilt ist. Da die datenschutzrechtliche Aufsichtsbehörde des Hessischen Rundfunks aber keine Kompetenzen für Beteilungen hat, wurde durch die entsprechende Verwaltungsvereinbarung der RDSK die **Degeto der Aufsicht des Rundfunkdatenschutzbeauftragten des NDR unterstellt**. Insbesondere aufgrund eines größeren Vorhabens der ARD-Anstalten, das bei der Degeto zusammengeführt wird, gab es daher im Berichtsjahr eine Prüfung:

Die Landesrundfunkanstalten planen die Errichtung einer IT-basierten Anwendung, in der Produzenten- und Urheberstammdaten verarbeitet werden, um auf Basis von Gemeinsamen Vergütungsregeln die Abrechnungen für berechtige

Urheber*innen und Leistungsschutzberechtigte vorzunehmen. Das Vorhaben ist komplex, weil eine Reihe von Daten verarbeitet werden und die unterschiedlichen Leistungsbeziehungen berücksichtigen werden müssen.

Das Vorhaben und die Umsetzung weiterer Anforderungen der DSGVO bei der Degeto wurden geprüft, Fortsetzung folgt.

d) Austausch mit der Datenschutzkonferenz

Auch im Jahr 2023 gab es zweimal virtuelle Treffen mit Mitgliedern der **Datenschutzkonferenz** (DSK), also dem Gremium der Datenschutzaufsichtsbehörden des Bundes und der Länder. Eingeladen waren auch die datenschutzrechtlichen Aufsichtsbehörden der Kirchen und des privaten Rundfunks.

Die Protokolle der Sitzungen veröffentlicht die DSK unter https://www.datenschutzkonferenz-online.de/protokolle.html.

Themen waren unter anderem

- der Beschluss der DSK „Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten“,
- die Überarbeitung des Kurzpapiers der DSK zur Zertifizierung nach Art. 42 DSGVO,
- die Entschließung zur „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz“,
- Kriterien für Souveräne Clouds,
- ein Bericht aus dem Europäischen Datenschutzausschuss,
- eine Leitlinie zur Zertifizierung als Instrument für Drittstaatenübermittlung,
- eine Leitlinie zu irreführenden Gestaltungsmustern in der Schnittstelle von Social-Media-Plattformen,
- eine Stellungnahme zu der Adäquanz-Entscheidung zum Data Privacy Framework und
- die Einrichtung einer Taskforce zum Thema ChatGPT.

Zudem gab es einen Austausch zur **Verbesserung der Kooperation** zwischen der DSK und den Datenschutzaufsichtsbehörden des Rundfunks und der Kirchen. Angeregt wurden einige grundsätzliche Änderungen in Bezug auf die Kommunikation in den Arbeitskreisen der DSK durch einen intensiveren Informationstransfer und eine **engere Einbindung**. Verabredet wurde ein Konzept zur Einbindung aller Datenschutzaufsichtsbehörden. Dazu soll u. a. auf der Homepage des BfDI eine Gesamtübersicht der Kontaktinformationen aller Datenschutzaufsichtsbehörden bereitgestellt und verlinkt werden. Die Redaktion und Aktualisierung soll durch die ZASt (Zentrale Anlaufstelle) erfolgen. Die ZASt koordiniert die grenzüberschreitende Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder mit den anderen Mitgliedstaaten der Europäischen Union, dem Europäischen Datenschutzausschuss (EDSA) und der Europäischen Kommission.

Wie tatsächlich der zukünftige Austausch ausgestaltet sein wird, bleibt abzuwarten. Die Mitglieder der RDSK und die datenschutzrechtlichen Aufsichtsbehörden der Kirchen sehen aufgrund der Fülle der Aufgaben und der Vielzahl der nicht-sektorspezifischen Themen, die für alle privaten und öffentlichen Einrichtungen aus datenschutzrechtlicher Perspektive einheitlich zu beurteilen sind (etwa Fragen des Beschäftigtendatenschutzes, Vorgaben für Auskunfts- und Transparenzpflichten, digitale Kommunikation, Einsatz von KI), **die Notwendigkeit einer engeren Verzahnung**.

In dem Entwurf zur Novellierung des Bundesdatenschutzgesetzes soll aufgrund des § 16a BDSG-E die DSK „institutionalisiert“ werden: „Die oder der Bundesbeauftragte im Sinne des § 8 sowie die Aufsichtsbehörden der Länder im Sinne des § 40 bilden die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Die Datenschutzkonferenz gibt sich eine Geschäftsordnung.“

Die DSK hat diesen Vorschlag zur Institutionalisierung zwar grundsätzlich begrüßt, die Formulierung im Einzelnen aber kritisiert, weil mit der so gefassten Vorschrift „eventuell andere nach Landesrecht vorgesehene sektorspezifische Datenschutzaufsichtsbehörden“ – also die des Rundfunks und der Kirchen – nicht aus der DSK ausgeschlossen wären (https://www.datenschutzkonferenz-

online.de/media/st/23_09_06_DSK_Stellungnahme_BDSG.pdf). Die Mitglieder der RDSK sind derzeit keine Mitglieder der DSK, gleichwohl ist über konstruktivere Formen eines Zusammenwirkens, z. B. durch Verfahrensregelungen, nachzudenken. Ebenso wie die EU-Kommission einen „**Vorschlag für eine Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679 (DSGVO)**“ vorgestellt hat, um die Zusammenarbeit von nationalen Behörden in grenzüberschreitenden Fällen zu erleichtern und beschleunigen, kann über entsprechende Verständigungen auch auf nationaler Ebene nachgedacht werden.

Weiterhin gab es eine Erörterung über die in Art. 52 Abs. 4 DSGVO geforderten, für die Erfüllung der gesetzlichen Aufgaben **notwendigen Ressourcen**, insbesondere der **Personalausstattung**, und deren Festlegung bzw. Evaluierung.

2. Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF, ORF, ARTE, DRadio und SRG SSR (AKDSB)

Der AKDSB hat sich in seinen regelmäßig durchgeführten Sitzungen und Videokonferenzen schwerpunktmäßig mit diesen Themen befasst:

- Aktuelle Entwicklungen in Rechtslage, Rechtsprechung und Politik
- Austausch zur Umsetzung der DSGVO in den Rundfunkanstalten
- Klagen auf Schmerzensgeld wegen angeblich unvollständigen Auskünften
- Art und Weise der Beantwortung von Auskunftsersuchen
- Etablierung von Datenschutzmanagementsystemen
- DSGVO-konforme Auftragsvergaben und Beschaffungen
- Einhaltung von Datenschutzgrundsätzen bei Auftragsprogrammierungen durch Dienstleister
- Einhaltung datenschutzrechtlicher Vorgaben bei einzelnen Verarbeitungstätigkeiten und IT-Systemen
- Beauftragung und Kontrolle beim Einsatz von Drittanbietern
- Harmonisierung von SAP-Anwendungen
- Nutzungsmessungen
- Datensicherheit und Cyberrisiken

- Datenschutzkonformer Einsatz von KI
- Konsequenzen aus dem Data Privacy Framework
- Beschaffung eines digitalen Hinweisgebersystems
- Homeoffice bei externen Dienstleistern
- Harmonisierungen und Überarbeitungen von Datenschutzerklärungen
- Wahrung des Datenschutzes bei Diversity-Umfragen
- Gemeinsames Login und Datenaustausch der Mediatheken von ARD und ZDF
- Live-Streaming und Aufzeichnung von Rundfunk- bzw. Fernsehratssitzungen

Zudem gibt es regelmäßig Termine der Datenschutzbeauftragten der Kooperationspartner des IVZ (Informations-Verarbeitungs-Zentrum von ARD und Deutschlandradio), in denen relevante Themen aus datenschutzrechtlicher Perspektive erörtert werden.

II. Tätigkeitsschwerpunkte bezüglich Datenverarbeitungen im NDR

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beschreibt seine Aufgaben wie folgt:

„Der BfDI – informieren, beraten, durchsetzen
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) verfolgt mit seinen Mitarbeiterinnen und Mitarbeitern das Ziel, den Datenschutz zu sichern und auszubauen. Er trägt damit zur notwendigen Autonomie aller Bürgerinnen und Bürger gegenüber Staat, Organisationen und Unternehmen bei. Seit 2006 kann sich zudem jeder an ihn wenden, der sein Recht auf Informationszugang nach dem Informationsfreiheitsgesetz (IFG) als verletzt ansieht“ (https://www.bfdi.bund.de/DE/DerBfDI/Inhalte/DerBfDI/DerBfDIinformierenberatendurchsetzen.html).

Ebenso stellen sich die Aufgaben des Rundfunkdatenschutzbeauftragten des NDR dar mit Blick auf den NDR, die Tochterunternehmen, Beteiligungsgesellschaften und sonstigen Verwaltungseinheiten. Die Reihenfolge „**informieren, beraten, durchsetzen**“ beschreibt nicht nur die Aufgaben, sondern auch die Prioritäten. Es geht maßgeblich da-

rum, durch frühzeitige und umfassende Information und Beratung den Verantwortlichen zu befähigen, datenschutzkonform zu agieren.

Damit in allen Verarbeitungsvorgängen von Anfang an datenschutzrechtliche Anforderungen beachtet werden, ist eine Einbeziehung des Rundfunkdatenschutzbeauftragten ratsam. Dies kommt sowohl dem Verantwortlichen als auch den betroffenen Personen zugute, weil damit von repressiven Aufsichtsmaßnahmen abgesehen werden kann, Verstöße mithin vermieden werden können, und das Recht auf informationelle Selbstbestimmung am besten gewahrt wird.

Die Aufgabenbereiche betreffen, wie in den Jahren zuvor auch, den gesamten Geschäftsbetrieb, also

- die Programmerstellung und -verbreitung,
- den Einzug der Rundfunkbeiträge,
- Beschäftigtendaten und weitere
- Organisations- und Strukturprojekte.

1. Zur Umsetzung der DSGVO

Die Überwachung der Einhaltung insbesondere der Vorgaben der DSGVO in allen Datenverarbeitungsvorgängen ist das Kerngeschäft. Die immer mehr durch die Rechtsprechung ausgeformten datenschutzrechtlichen Vorgaben müssen in der Unternehmenspraxis umgesetzt werden. Dazu können technische und/oder organisatorische Maßnahmen eingesetzt werden. Einzelfallbezogen sind entsprechende Vorkehrungen zu prüfen und umzusetzen. Der Erwägungsgrund 78 der DSGVO beschreibt diese Anforderung gut nachvollziehbar: „Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin

bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. […]“

Dass dies eine für den Verantwortlichen und die zuständige Aufsichtsbehörde fortwährende und immer neuen Anforderungen unterliegende Aufgabe ist, dürfte aufgrund der Dynamik der technisch geprägten Veränderungsprozesse nachvollziehbar sein.

2. Programm und Programmverbreitung

Der Besuch einer Internetseite führt zu Datenverarbeitungen. Externe Anfragen und Beschwerden zu diesem Verbreitungsweg der Angebote des NDR werden daher vorrangig eingereicht.

a) Datenschutzerklärungen und Informationspflichten

Die Datenschutzerklärungen sind im Wesentlichen unverändert geblieben. Aufgrund von Änderungen bei der Beauftragung von Dienstleistern und neuen Angebotsinhalten gab es allerdings Anpassungen und Ergänzungen. Die Gebote der Vollständigkeit, Transparenz und Verständlichkeit der Informationspflichten können als erfüllt angesehen werden, auch wenn teilweise noch Neuerungen vorzunehmen sind. Insbesondere zur Nutzung von Drittplattformen und Reichweitenmessung sind Aktualisierungen vorzunehmen. Bezüglich des zuletzt genannten Themas wurde daher dem Verantwortlichen ein Fragebogen übermittelt, der Gewissheit über die eingesetzten Tools verschaffen und zu klareren Ausführungen in den Datenschutzerklärungen führen soll, damit die genannten Anforderungen besser nachvollziehbar werden.

b) Anfragen zu den Angeboten und Datenschutzerklärungen des NDR

Im Berichtsjahr 2023 gab es kaum Änderungen hinsichtlich des Inhalts der Anfragen und Beschwerden. Wie zuvor auch, betrafen die rund 30 Zuschriften

- allgemeine Nachfragen zu den Datenschutzbestimmungen und deren Geltungsbereich
- die Rechtsmäßigkeit der Nutzungsmessungen
- Embedding
- Einwilligungserfordernisse
- Datenschutzbestimmungen für Foren und
- technische Funktionalitäten, Serverdienste
- die Nutzung von Drittplattformen
- Personalisierungen.

Relevant waren insbesondere diese Themen:

Es ist sicherlich eher unüblich, dass Telemedienangebote genutzt werden können, ohne zuvor eine Auswahl über Datenverarbeitungen mittels **Cookie-Banner** zu treffen. In aller Regel werden beim Besuch einer Internetseite Konfigurationsmöglichkeiten angeboten, etwa um Zustimmungen zu Nutzungsmessungen oder die Weitergabe von Daten an verbundene Unternehmen einzuholen. Die vom NDR verantworteten Telemedienmedienangebote kommen derzeit ohne entsprechende Cookie-Banner aus, was zu Nachfragen und Beschwerden führt. Die Rechtslage hat sich allerdings insoweit nicht verändert. Im vergangenen Bericht wurde bereits ausgeführt, dass die Einholung einer Einwilligung für „funktionale“ (erforderliche) Cookies nicht eingeholt werden muss. Erforderlich sind beispielsweise Cookies, die eingesetzt werden für

- eine technische Fehleranalyse,
- die Gewährleistung der technischen Sicherheit des Angebots oder
- die Darstellung und Individualisierung von Inhalten.

Zu diesen erforderlichen Verarbeitungen zählt jedoch auch **die Erhebung von anonymen, statistischen Nutzungsdaten**, jedenfalls soweit der publizistische

Auftrag des öffentlich-rechtlichen Rundfunks betroffen ist. Die Rundfunkanstalten haben ein berechtigtes und notwendiges Interesse an der Erhebung, wie ihre Angebote genutzt werden. Der Einsatz von entsprechenden Cookies oder vergleichbaren Messmethoden zur Akzeptanz der Angebote darf daher ohne Einwilligungen erfolgen. **Eine ausschließlich publizistisch motivierte anonymisierte Nutzungsmessung ist daher auch ohne vorherige Zustimmung mit den einschlägigen rechtlichen Vorgaben und der aktuellen Rechtsprechung vereinbar** (Art. 6 Abs. 1 DSGVO i.V.m. § 30 Abs. 3 Medienstaatsvertrag). Auch nach Maßgabe des § 25 Abs. 1 TTDSG (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien) ergibt sich kein anderes Ergebnis. Danach ist es ebenfalls dem Verantwortlichen möglich, die ausschließlich anonymisierte Nutzungsmessung zu publizistischen Zwecken durchzuführen, ohne eine Einwilligung einzuholen. Denn die entsprechende Datenverarbeitung dient dem Zweck der Erfüllung des Funktionsauftrags des öffentlich-rechtlichen Rundfunks zur Positionierung im publizistischen Wettbewerb. Anders kann dies aber zu beurteilen sein, wenn bloße Informationen zu Verwaltungstätigkeiten in eigenen Internetangeboten dargeboten werden, da es insoweit an einer publizistischen Motivation fehlt.

Embedding meint das Einbinden oder Einbetten von externen Inhalten in das eigene Telemedienangebot. Derartige Vernetzungen sind allseits üblich. Die Einbettungen lösen üblicherweise Datenverarbeitungen aus und sind daher aus technischen Gründen und solchen der Transparenz entsprechend zu gestalten und zu kennzeichnen. In einigen Fällen hat der Verantwortliche **vertragliche Lösungen** für ein rechtskonformes Embedding geschaffen, in anderen Fällen war über **entsprechende Informationen für die Nutzenden und technische Lösungen** eine datenschutzkonforme Gestaltung möglich. Die zu diesen Angelegenheiten eingegangen Beschwerden wurden nach den genannten Maßgaben geprüft und beantwortet. Verstöße gegen datenschutzrechtliche Anforderungen waren nicht festzustellen.

Auch wenn die vom NDR verantworteten Telemedienangebote ohne **Einwilligungen** genutzt werden können, sind für einige Angebotsinhalte Einwilligungen einzuholen. Regelmäßig werden bei der Teilnahme an Gewinnspielen

oder der Nutzung von Chats, Foren usw. personenbezogene Daten verarbeitet, und zwar beispielsweise

- E-Mail-Adressen,
- (Nutzer*innen-) Namen,
- die Beiträge der Nutzenden und
- Log-In-Daten.

Dafür muss zumindest konkludent durch die Teilnahme oder Registrierung eine Einwilligung eingeholt werden. **Konkludente Einwilligungen der Nutzenden für die Veröffentlichung ihrer Beiträge in Chats und Foren** sind hinreichend, weil die Äußerungen Teil des journalistischen Angebots werden und dem Medienprivileg zuzurechnen sind. In diesem Sinne konnten die Anfragen beantwortet werden.

Auch die rechtliche Zulässigkeit der Nutzung von **Facebook und anderen kommerziellen Drittplattformen** als Verbreitungsweg für Programminhalte war wiederum ein Thema. Die entsprechende gerichtliche Auseinandersetzung des Bundespresseamtes und dem Bundesbeauftragten für den Datenschutz und die Informationssicherheit wurde bereits erwähnt (D. II. 1.). Ob und gegebenenfalls welche Konsequenzen aus einem eines Tages rechtskräftigen Urteil für den öffentlich-rechtlichen Rundfunk zu ziehen sind, steht noch aus. Es gibt jedoch gute Gründe, die Nutzung entsprechender Plattform **aus journalistischen Gründen** als datenschutzrechtlich zulässig anzusehen. Der Funktionsauftrag des öffentlich-rechtlichen Rundfunks und die zur Erfüllung der Aufgaben anfallenden Datenverarbeitungen überwiegen nach hiesiger Auffassung dem Zweck der Datenverarbeitung, die Art. 6 Abs. 1 lit. e), Abs. 3 Satz 4 DSGVO fordert. Je nach Datenverarbeitung der entsprechenden Plattform kann es zu einer Kollision der Rundfunkfreiheit einerseits und der informationellen Selbstbestimmung der nutzenden Personen kommen. Diese beiden verfassungsrechtlich geschützte Rechtsgüter sind möglichst in Einklang zu bringen. Das Abschalten entsprechender Präsenzen ginge jedenfalls einseitig zu Lasten der Rundfunkfreiheit, obgleich dort viele Personen erreicht werden (wollen). Vorzugswürdig ist, durch entsprechende Informatio-

nen und Transparenzmaßnahmen auf die Datenverarbeitungen zu verweisen und keine exklusiven Inhalte auf Drittplattformen zu veröffentlichen.

Ganz überwiegend wohlwollend und um die **Persönlichkeitsrechte** anderer Protagonist*innen besorgt, gab es einige Hinweise und Anfragen, ob die Abbildung von Personen oder Datenbeständen mit sensiblen Inhalten datenschutzrechtlichen Vorgaben entspricht. Aber auch das „Recht auf Vergessenwerden“ wurde eingefordert. Die geprüften Sachverhalte waren im Ergebnis nicht zu beanstanden. **Personen dürfen grundsätzlich nur mit deren Einwilligung verbreitet werden**. Entsprechende Erklärungen lagen dem NDR auch vor. Ohne eine Einwilligung darf eine Person nur dann gezeigt werden, wenn es sich um Bildnisse aus dem Bereich der Zeitgeschichte oder Bilder handelt, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen. Dies gilt auch für Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben (§ 23 KUG).

c) Anfragen von Redaktionen

Die Aufgabe der Beratung wurde auch aufgrund entsprechender Anliegen im redaktionellen Bereich erfüllt. Aufgrund des sogenannten Medienprivilegs gibt es zwar Ausnahmen vom Datenschutz im journalistischen Bereich, da Informations- und Dokumentationspflichten, Auskunfts- und Widerrufsrechte für Betroffene nicht gelten. Weitere Anforderungen, wie etwa die der Zweckbindung, Datensparsamkeit und Datensicherheit bleiben aber bestehen. Die **Reichweite des Medienprivilegs** ist einzelbezogen zu bestimmen. Beraten wurde zum Beispiel bezüglich

- datenschutzrechtlichen Anforderungen in Communities
- Änderungen beim gemeinsamen Login der Mediatheken von ARD und ZDF
- der Rekrutierung von Test- und Feedbackgruppen
- Modalitäten für die Anmeldung für das Bürgerparlament
- Akkreditierungsanfragen
- Datenschutzfragen zum ESC

- allgemeinen Anfragen zu neuen Programmformaten
- Datenerhebungen beim Publikum
- sicheren Ablageorten für Daten von Teilnehmer*innen von Programmaktionen
- Anforderungen an Community-Management-Systeme
- Datenschutzhinweise für Studienteilnehmer*innen
- Gestaltung von Bewerbungsformularen
- der Beschreitung neuer Verbreitungswege (Mastodon, Verbreitung von Nachrichten über Messenger-Dienste)

Regelmäßig war neben anderen Anforderungen darauf zu verweisen, dass der Verantwortliche nur solche Daten als Pflichtangaben erheben darf, die für den konkreten Zweck (Teilnahme an einer Programmaktion, Kontaktaufnahme, Mitgliedschaft in einer Community) unbedingt erforderlich sind. Sofern weitere personenbezogene Daten abgefragt werden sollen, muss ein Hinweis erfolgen, dass dies nur im Rahmen der Freiwilligkeit passiert. Auch eine etwaige Weitergabe der an Dritte (etwa Dienstleister, die einen Gewinn auskehren) muss kommuniziert werden. Weiterhin ist vorab festzulegen, wie lange welche Daten zu welchem Zweck aufbewahrt werden.

Neben der Beratungstätigkeit in Einzelfällen soll zukünftig der **Austausch mit den Redaktionen im NDR** intensiviert werden. Zwar gibt es seit dem Jahr 2022 eine Verständigung im NDR, dass alle Beschäftigten – unabhängig vom Status und dem Ort ihrer Tätigkeit – jährlich wiederkehrend Online-Schulungen zum Datenschutz und der IT-Sicherheit absolvieren. Gezeigt hat sich in diesem Berichtsjahr aber, dass ein zusätzlicher Austausch über spezifische datenschutzrechtliche fruchtbar ist, um (redaktionelle) Besonderheiten zu erörtern.

3. Rundfunkteilnehmerdatenschutz

Gemäß § 11 Absatz 2 Rundfunkbeitragsstaatsvertrag haben die Landesrundfunkanstalt den Beitragsservice mit der Durchführung des Rundfunkbeitragseinzugs und der Ermittlung von Beitragsschuldnern beauftragt. Daher ist beim Beitragsservice auch eine behördliche Datenschutzbeauftragte zu bestellen. Allgemeine

Anliegen des Beitragsrechts aus datenschutzrechtlicher Perspektive fallen daher in die dortige Zuständigkeit. Neben der Prüfung und Überwachung der Einhaltung datenschutzrechtlicher Vorgaben ist die Aufgabe des Rundfunkdatenschutzbeauftragten des NDR die Bearbeitung von **Beschwerden**, soweit der NDR betroffen ist. Regelmäßig gehen daher Beschwerden ein, die den **Umfang der verarbeiteten Daten, die Weitergabe von Daten an Dritte oder Fragen des Auskunftsrechts** betreffen.

Im Jahr 2021 gab es beim Beitragsservice 1.116 Auskunftsersuchen, die den NDR betrafen. Im Jahr 2022 waren es 939 und im aktuellen Berichtsjahr 1622. Die Anzahl hat sich damit stark erhöht.

Beim NDR in Hamburg sind 25 allgemeine Auskunftsanfragen eingegangen und 13 Ersuchen, die ausschließlich den Beitragseinzug durch den NDR betrafen. Insoweit gab es keine wesentlichen Schwankungen. Dies gilt auch hinsichtlich der eingereichten rund 30 Beschwerden. Zu zwei regelmäßig wiederkehrenden Beschwerdeinhalten soll an dieser Stelle kurz ausgeführt werden:

Die aktuelle Rechtsprechung zum Auskunftsanspruch des Art. 15 DSGVO wurde oben dargestellt (D. II. 3.). **Der Auskunftsanspruch hinsichtlich der zum Zwecke des Rundfunkbeitragseinzugs** verarbeiteten personenbezogenen Daten richtet sich nach § 11 Absatz 8 Rundfunkbeitragsstaatsvertrag (RBStV). Diese Vorschrift lautet:

„Jede natürliche Person hat das Recht, bei der für sie zuständigen Landesrundfunkanstalt oder der nach § 10 Abs. 7 eingerichteten Stelle Auskunft zu verlangen über

1. die in § 8 Abs. 4 genannten, sie betreffenden personenbezogenen Daten,
2. das Bestehen, den Grund und die Dauer einer sie betreffenden Befreiung oder Ermäßigung im Sinne der §§ 4 und 4 a,
3. sie betreffende Bankverbindungsdaten und
4. die Stelle, die die jeweiligen Daten übermittelt hat.

Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder aus-

schließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, sind vom datenschutzrechtlichen Auskunftsanspruch nicht umfasst."

Auskünfte, die nach dieser Maßgabe erteilt werden, sind insoweit als vollständig anzusehen. Die Rundfunkanstalten bzw. der in ihrem Auftrag handelnde Beitragsservice haben, soweit es um die Feststellung der Pflicht zur Zahlung des Rundfunkbeitrags sowie die Abwicklung der damit verbundenen Verwaltungsverfahren geht, die für sie maßgeblichen formellen und materiellen Gesetze anzuwenden, solange und soweit sie nicht für ungültig bzw. unwirksam erklärt worden sind. Eine solche Feststellung ist mit Bezug auf Gesetze im formellen Sinne den Verwaltungsgerichten, in Bezug auf Gesetze im materiellen Sinne hingegen ausschließlich dem Bundesverfassungsgericht oder – soweit es um die Vereinbarkeit mit verbindlichem Europarecht geht – dem Europäischen Gerichtshof vorbehalten. Die eingangs genannten Entscheidungen zur Auslegung des Artikel 15 DSGVO machen zur Spezialvorschrift für den Beitragseinzug keine Aussagen. **Die gegen den Umfang der nach § 11 RBStV erteilten Auskünfte eingereichten Beschwerden hatten daher keinen Erfolg**. Warum die Auskünfte nach dieser Spezialvorschrift erteilt werden, hat der Gesetzgeber in der Begründung zum 21. Rundfunkänderungsstaatsvertrag erläutert:

„Die Landesrundfunkanstalten verarbeiten zum Zwecke des Beitragseinzugs Daten der Beitragsschuldner. Hierbei handelt es sich nicht um eine Datenverarbeitung zu journalistischen Zwecken im Sinne des Artikels 85 der Datenschutzgrundverordnung. Indes sieht bereits die Datenschutzgrundverordnung selbst weitere Einschränkungen vor, wenn sich die Datenverarbeitung für den Verantwortlichen als rechtliche Verpflichtung darstellt (Artikel 6 Abs. 1 Buchst. c) oder durch Rechtsvorschriften ausdrücklich geregelt ist (Artikel 14 Abs. 5 Buchst. c). Ebenso können die Mitgliedsstaaten Beschränkungen vornehmen, wenn dies zum Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses, etwa im Abgabenbereich erforderlich ist (Artikel 23 Abs. 1 Buchst. e). **Die Datenverarbeitung zum Zwecke des Beitragseinzugs stellt ein solches wichtiges Ziel des allgemeinen öffentlichen Interesses dar**, denn sie dient dazu, die verfassungsrechtlich garantierte, funktionsgerechte Finanzausstattung des öffentlich-rechtlichen Rundfunks sicherzustellen."

Wenn Rundfunkbeiträge nicht geleistet werden, ergehen entsprechende Zahlungsaufforderungen und Beitragsbescheide an die beitragspflichtige Person. Sofern auch dann keine Zahlungen geleistet werden und Vollstreckungen erfolglos bleiben, kann die **Beitreibung offener Forderungen an Dritte übertragen** werden. Eine entsprechende gesetzliche Grundlage findet sich in der „Satzung des NDR über das Verfahren zur Leistung der Rundfunkbeiträge“ (§ 16 Absatz 1 regelt die Übertragung einzelner Tätigkeiten auf Dritte (Auftragnehmer).

Die **Weitergabe entsprechender Daten an Dritte zur Geltendmachung offener Beitragsforderungen verstößt daher grundsätzlich nicht gegen datenschutzrechtliche Vorgaben**, weil sie auf einer rechtlichen Grundlage erfolgt. Das Recht, eine derartige Satzung zu erlassen und die Weitergabe der Daten vorzunehmen, leitet sich wiederum aus den entsprechenden Bestimmungen des Rundfunkbeitragsstaatsvertrages ab (§ 10 Absatz 7): „Die Landesrundfunkanstalt ist ermächtigt, einzelne Tätigkeiten bei der Durchführung des Beitragseinzugs und der Ermittlung von Beitragsschuldnern auf Dritte zu über-tragen und das Nähere durch die Satzung nach § 9 Abs. 2 zu regeln.“

Die gegen eine entsprechende Weitergabe von Daten gerichteten Beschwerden blieben daher erfolglos.

4. Beschäftigtendatenschutz

Der Schutz von personenbezogenen Daten der Beschäftigten war wiederholt Gegenstand von Beratungen und Anfragen.

a) Schulungen

Auszubildende und Volontä*innen werden beim Eintritt in den NDR persönlich in datenschutzrechtlichen Belangen und solchen der IT-Sicherheit geschult. Daneben gab es zu einzelnen Bereichen Informationstermine zu datenschutzrechtlichen Themen, die zukünftig intensiviert werden sollen, da die verpflichtenden Online-Schulungen auf die Vermittlung von Grundsätzen beschränkt sind.

b) Interne Regelwerke

Eine Reihe von technischen Anwendungen werden begleitend mit eigenen Regelwerken versehen, um Risiken bei der Verarbeitung von personenbezogenen Daten zusätzlich organisatorisch abzusichern. Bei der Einführung neuer Anwendung entfaltet sich daher ein entsprechender Beratungsbedarf, aber auch bei der Überarbeitung bestehender Regelwerke. Diese Aufgabe ist von Dauer, weil technische Entwicklungen und veränderte Geschäftsprozesse abgebildet werden müssen. Dienstvereinbarungen, Dienstanweisungen und sonstige Richt- und Leitlinien sind daher zu entwickeln und anzupassen.

c) Löschungen von Daten

Insbesondere bei älteren elektronischen Anwendungen war zumindest nicht automatisiert die Vorgabe der sogenannten **Speicherbegrenzung** implementiert. Diese Vorgabe des Art. 5 Absatz 1 lit. e) DSGVO meint, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleiben muss. Der Verantwortliche muss daher entsprechende Prozesse aufsetzen oder weitere Tools einsetzen, um Löschungen von Daten vorzunehmen. Entsprechende Vorhaben waren zu beraten und zu begleiten.

d) Datenschutz und Personalplanungen

Die Verarbeitung von Beschäftigtendaten kann nicht nur zur Abwicklung des jeweiligen Arbeitsverhältnisses vorgenommen werden, sondern auch zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes. Diesbezüglich gab es ein Vorhaben zu beraten, das sich mit dem Aufbau einer internen Jobbörse beschäftigt, in der Daten von freien Mitarbeitenden verarbeitet werden. Die Grundlagen und einzelne konkrete Fragen dazu wurden erörtert.

e) Wahlen, Abstimmungen, Umfragen

Der Bedarf an elektronischen Anwendungen zum Zwecke der Durchführung von Wahlen, Abstimmungen und Umfragen ist unverändert hoch und hat sogar zugenommen. Problematisch war und ist das Versprechen der Anonymität unter den Teilnehmenden. Für die drei genannten Zwecke konnte daher kein einheitliches Tool ausgemacht werden, welches die Nichtrückführbarkeit der Antworten auf bestimmte Personen garantiert. Immerhin konnten aber unter Abschichtung der Anliegen und mit organisatorischen Regellungen für einige Anwendungszwecke Lösungen entwickelt werden.

f) Diversity-Umfrage

Die Landesrundfunkanstalten planen, eine sogenannte Diversity-Umfrage unter ihren Beschäftigten durchzuführen. Ob und wie diese Umfrage durchgeführt wird, ist noch offen. Das Projekt wird diesseits als kritisch angesehen, weil Daten abgefragt werden sollen, die in einem Bewerbungsgespräch und in einem Arbeitsverhältnis „nichts zu suchen“ haben, etwa Herkunft (der Eltern), Religionszugehörigkeit, geschlechtliche Identität, sexuelle Orientierung, Diskriminierungserfahrungen. Die Fragen betreffen mithin zum großen Teil besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO. Die Zulässigkeit einer solchen Umfrage wird mithin maßgeblich daran hängen, ob tatsächlich die Freiwilligkeit und Anonymität gewährleistet sein werden. Eine abschließende Prüfung konnte nicht vorgenommen werden, weil die einzelnen technischen Verarbeitungsprozesse noch nicht geklärt waren.

g) Missbräuchliche Nutzung der IT-Ausstattung des NDR

In seltenen Fällen kommt es vor, dass die IT-Ausstattung des NDR in einer Weise genutzt wird, die den internen Vorgaben widerspricht. Grundsätzlich ist es den Beschäftigten gestattet, die IT des NDR nur in einem geringen Umfang privat zu nutzen, so dass die Belange des NDR (das Ansehen, die Reputation, die dienstlichen Verpflichtungen der Beschäftigten) nicht tangiert werden. Ausnahmsweise wurde gegen diese Vorgaben verstoßen, so dass ein entspre-

chendes Verfahren greift, um den Sachverhalt aufzuklären und gegebenenfalls Maßnahmen zu ergreifen. Es hat sich in diesen Fällen als vorteilhaft herausgestellt, dass der NDR die angeratene Empfehlung, eine private Nutzung des dienstlich zur Verfügung gestellten E-Mail-Accounts nicht zuzulassen, umgesetzt hat. Dadurch werden Schwierigkeiten vermieden, mit denen sich etwa das Landesarbeitsgericht Baden-Württemberg beschäftigen musste (s. o. unter D. II. 4.).

h) Arbeitszeiterfassung

Aufgrund entsprechender höchstrichterlicher Entscheidungen muss die Arbeitszeit von Beschäftigten vom Arbeitgeber erfasst werden. Zunächst hatte der EuGH geurteilt, dass die Mitgliedstaaten die Arbeitgeber verpflichten müssen, ein objektives, verlässliches und zugängliches System zu etablieren, in welchem die täglich geleistete Arbeitszeit der beschäftigten Personen dokumentiert wird (EuGH, Urteil vom 14.05.2019, Rs. 55/18 CCOO). Sodann entschied das Bundesarbeitsgericht (Urteil vom hat am 13.09.2022, Az. 1 ABR 22/21) ebenso, dass die Arbeitgeber zum einen zur Einführung eines Systems zur Arbeitszeiterfassung verpflichtet sind, zum anderen muss aber auch sichergestellt werden, dass von dem entsprechenden System auch tatsächlich Gebrauch gemacht wird. Im Berichtsjahr hat der NDR einen Auftakt zur Einführung eines solchen Systems gemacht, mit der tatsächlichen Einführung ist im Jahr 2024 zu rechnen. Die eingehenden datenschutzrechtlichen Fragen werden also noch folgen.

5. Weitere Beratungen und Prüfungen im NDR

Wie bereits erwähnt, besteht die Aufgabe des Rundfunkdatenschutzbeauftragten maßgeblich in der Überwachung der Einhaltung der Vorgaben der DSGVO in allen Datenverarbeitungsvorgängen des Verantwortlichen. Damit dies am besten gelingt, wird in der Regel frühzeitig über Projekte und Vorhaben informiert, damit Beratungsleistungen wirksam erbracht werden können. Eine Reihe von Projekten zielt darauf ab, Geschäfts- und Produktionsvorgänge zu digitalisieren, zu erneuern oder zu ersetzen. Es handelt sich um unterschiedliche Anwendungen und Prozesse aus allen Bereichen des NDR, auszugsweise etwa

- digitale Buchungstools
- Einsatz von biometrischen Daten
- crossmediale Suchmaschinen
- Nutzung von Cloud-Anwendungen
- Umsetzung und Auswertung des Desksharings
- internetbasierte Medienproduktionen
- Besonderheiten der Medienproduktion im Ausland
- technische Ausstattung von Auslandsstudios
- Ersatz von Sendetechniken und senderelevante Ausstattungen
- Technikersatz bei Produktionsarbeitsplätzen
- digitalisierte Zeiterfassungen
- Weiterentwicklung von Kollaborations- Kommunikationstools
- Einführung (Digitalisierung) von elektronische Akten
- Elektronische Unfallmeldesysteme
- Sonstige neue Fachapplikationen und Ablösungen von Software

Insgesamt waren über 100 kleinere und größere Anwendungen und Projekte zu begleiten und prüfen. Regelmäßig werden durch die Projekte und Vorhaben Beschaffungsvorgänge ausgelöst. Der AKDSB und die IT-Sicherheitsbeauftragten der Rundfunkanstalten hatten daher gemeinsam Leitlinien entworfen, um die Einhaltung der Vorgaben des Datenschutzes und der Informationssicherheit bei Beschaffungsvorgängen von Anfang sicherzustellen. Die entsprechenden Vorgaben, die bei allen Beschaffungen gelten, liegen dem Verantwortlichen in einem entsprechenden Empfehlungspapier vor, dass den Prozess und die maßgeblichen Regelungen zusammenfasst („**Datenschutz und Informationssicherheit bei Beschaffungsvorgängen**“).

a) Künstliche Intelligenz

Im Laufe des Jahres hatte der NDR einen Prozess aufgesetzt, um den Einsatz von KI für unterschiedliche Geschäftszwecke zu prüfen und evaluieren. Es gab daher Anlass, frühzeitig auf etwaige Risiken hinzuweisen und inhaltliche und formale datenschutzrechtliche Vorgaben – auch für die Erprobung von KI-Anwendungen – aufzustellen.

Risiken und Probleme derartigen Anwendungen stellen sich regelmäßig aus diesen Gründen:

- Mangelnde Transparenz: Aus welchen Quellen stammen die Daten, auf die die Systeme zurückgreifen?
- Mangelnde Informationen: Auf welcher Rechtsgrundlage werden die Daten verarbeitet?
- Werden die Informationspflichten von betroffenen Personen erfüllt?
- Können betroffene Personen ihre Rechte auf Auskunft, Berichtigung und Löschung wirksam ausüben?
- Ist die Sicherheit der verarbeiteten Daten gewährleistet?
- Wo werden die Daten verarbeitet?
- An welche weiteren Unternehmen werden die Daten weitergegeben?
- (Wie) Werden Daten von Kindern geschützt?

Der Einsatz von KI muss daher auch zu Testzwecken nach Regeln erfolgen, die diese Risiken hinreichend und wirksam berücksichtigen. So ist etwa bei der redaktionellen Arbeit darauf zu achten, dass die eingesetzten Systeme die Einhaltung des Datengeheimnisses nicht gefährden und den Grundsatz der Vertraulichkeit und Integrität zur Gewährleistung der Datensicherheit nicht verletzen. Die in die KI-Anwendungen eingespeisten Inhalte dürfen daher beispielsweise nicht vertraulich sein. Auch muss der Informantenschutz gewahrt bleiben. Beim Einsatz von KI sind die Programmgrundsätze zu wahren. Auch bei KI-generierten Programmangeboten gilt die journalistische Sorgfaltspflicht.

Aber auch beim Einsatz von KI für unternehmensinterne Zwecke, also in der Verwaltung, bei der Verarbeitung von Beschäftigtendaten etc., war aufgrund der genannten Risiken darauf zu verweisen, dass mit öffentlich zugänglichen Daten, nicht aber mit internen Unternehmensdaten, Tests durchgeführt werden können. Auch war von einer automatisierten Verknüpfung von KI mit anderen bereits eingesetzten Anwendungen abzuraten.

b) Datensicherheit

Die Sicherheit von Daten und Informationen ist und bleibt im Allgemeinen ein Thema mit großer Relevanz. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht die Bedrohungslage in Deutschland als unverändert angespannt bis kritisch an. Die Bedrohung im Cyberraum sei so hoch wie nie zuvor (Bericht des BSI: „Die Lage der IT-Sicherheit in Deutschland 2023“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=6).

Der NDR setzt daher sowohl technische als auch organisatorische Maßnahmen ein, um die Risiken abzufangen. Dazu zählen u. a. sogenannte Phishing Schulungen, in denen die Beschäftigten trainiert werden, Angriffsmuster besser zu erkennen. Um die Wirksamkeit der Maßnahmen zu erhöhen, kommt es zu einer Verarbeitung personenbezogener Beschäftigtendaten. Dies hat teilweise Zweifel an der Rechtmäßigkeit des Vorhabens geweckt. Allerdings handelt der Verantwortliche dabei in einem berechtigtem Interesse im Sinne des Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Dies deshalb, weil nach dem Erwägungsgrund 49 der DSGVO Folgendes gilt:

„Die Verarbeitung von personenbezogenen Daten […] stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service“-Angriffe)

und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren."

Diese Erwägungen des Gesetzgebers dürften gerade vor dem Hintergrund der angespannten Sicherheitslage nachvollziehbar sein.

F. Informationszugang

Im Berichtsjahr wurden 18 Anträge auf Informationszugang an den NDR gerichtet; dreimal mehr als im Vorjahr. „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" (§ 47 Absatz 11 NDR Staatsvertrag). Von diesem Recht haben im Berichtsjahr zwei Personen Gebrauch gemacht. Vorgetragen wurde, dass der begehrte Antrag auf Informationen nicht umfänglich erfüllt worden sei. Ergebnis der Prüfung war, dass die Mehrzahl der gestellten Fragen umfassend beantwortet war. Allerdings war nicht in allen Fällen der erteilten Auskunft zu entnehmen, welcher ob und gegebenenfalls welcher Ablehnungsgrund für einzelne Fragen einschlägig gewesen sein soll. Es sollte im Falle einer Ablehnung mitgeteilt werden, nach welcher Norm abgelehnt wurde und jeweils eine Begründung erfolgen. Dies wurde erörtert und nachgeholt.

G. Fazit und Ausblick

Wie in den Jahren zuvor auch, waren im aktuellen Berichtsjahr zahlreiche Geschäftsprozesse aus datenschutzrechtlicher Perspektive in den Blick zu nehmen. Die Entwicklungen sind und bleiben auch immer eine Herausforderung für den Datenschutz. Um die Sensibilität für diese Belange zu stärken, sollen zukünftig vermehrt einzelne Geschäftsbereiche in den Blick genommen werden und die Anzahl der Informationsveranstaltungen erhöht werden. Auch gilt es, die Schaffung und Aktualisierung von internen Regularien intensiv zu beraten.

In welcher Weise KI als Arbeitsmittel in den NDR Einzug erhalten wird, bleibt noch abzuwarten. Die Erprobungsphasen einzelner Anwendungen dürfte demnächst abgeschlossen sein. Die Dynamik auf diesem Gebiet wird allerdings zu einer fortwährenden Beschäftigung mit dieser Thematik führen. Welche Aufgaben KI übernimmt, wie mächtig sie sein wird und wie sich durch ihren Einsatz die Arbeitsprozesse verändern, wird sich noch zeigen. Dies gilt auch hinsichtlich etwaiger Gefahren für Demokratien mit ihren konstituierenden freien Informationsangeboten.

Vor fast 200 Jahren, im Jahr 1825, wurde in England die erste Bahnstrecke für die Öffentlichkeit in Betrieb genommen. Die Skepsis und auch Angst vor diesem damals revolutionärem Verkehrsmittel hielt sich trotz ihrer raschen Verbreitung über viele Jahre. Befürchtet wurden Erkrankungen durch die Nutzung der Bahn – die sogenannte Eisenbahnkrankheit – aufgrund der „hohen“ Geschwindigkeiten von rund 30 km/h. Neue Techniken begeistern, werden belächelt oder gefürchtet bis hin zum Untergang von allem („KI-Doom“). „Lasst uns an die Stelle von Zukunftsängsten das Vordenken und Vorausplanen setzen“, riet einst Winston Churchill. Dies ist auch in diesem Zusammenhang ein guter Rat.