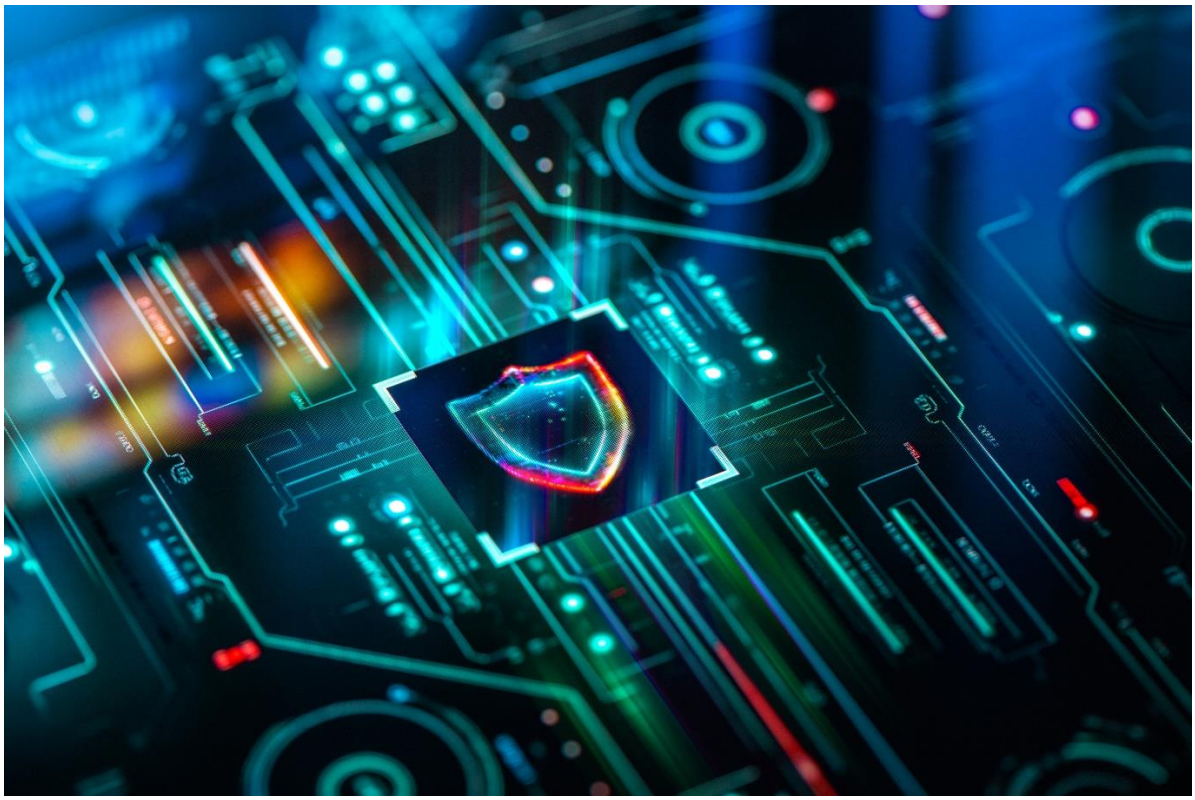
NORDDEUTSCHER RUNDFUNK

Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten des NDR

für das Berichtsjahr 2024

Dr. Heiko Neuhoff

Hamburg im Januar 2025



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 2024.

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 Jahr 1972 (!) legte der Hessische Datenschutzbeauftragte seinen ersten Tätigkeitsbericht vor. Das Land Hessen war zu dieser Zeit Vorreiter in Sachen Datenschutz und hatte das erste Datenschutzgesetz überhaupt erlassen. Dieser allererste Tätigkeitsbericht dieser Art ist auch 53 Jahre später erstaunlich aktuell. So heißt es dort beispielsweise:

„Die rasche Fortentwicklung der modernen Industriegesellschaft macht in immer stärkerem Maße eine umfassende planerische Vorsorge notwendig. […] Um richtige Entscheidungen fällen zu können, benötigt die Verwaltung möglichst umfassende Informationen, d. h. die Qualität ihrer Entscheidungen ist in erster Linie abhängig von der Quantität und Qualität der verfügbaren Informationen. Das große Problem für jede Verwaltung ist deshalb der Informationsfluß, denn veraltete, unvollständige und fehlerhafte Informationen können zu Fehlentscheidungen mit unter Umständen katastrophalen Folgen führen. […] Zur Erfassung, Speicherung und Verarbeitung von Informationen bedient sich die Verwaltung daher in zunehmendem Umfang der elektronischen Datenverarbeitung. Sie ermöglicht bei zweckentsprechender Organisation einen schnellen Fluß und eine umfassende, exakte und gezielte Auswertung der Informationen. Sie macht den Verwaltungsablauf sicherer, wirtschaftlicher und transparenter. Diese moderne Informationstechnik ist ein Hilfsmittel für die Verwaltung. Es gibt ihr die Möglichkeit zu schnellen und sachlich qualifizierten Entscheidungen für ihr operatives und planerisches Handeln."

Neben diesen fast euphorischen Ausführungen zur elektronischen Datenverarbeitung wurden auch die Risiken benannt:

„Die maschinelle Datenverarbeitung liefert der öffentlichen Verwaltung nicht nur verbesserte Informationen; sie schafft auch neue Möglichkeiten des Informationsmißbrauchs. Es muß deshalb sichergestellt sein, daß

1. das Persönlichkeitsrecht des Bürgers berücksichtigt und nur soviel Informationen über ihn gespeichert werden, wie die Verwaltung für ihre Entscheidungen benötigt,
2. die Datenbestände vor unberechtigten Zugriffen und Veränderungen geschützt sind […]."

Diese Grundsätze – Datensparsamkeit und Datensicherheit – gelten bis heute und sind sogar europa- und verfassungsrechtlich verankert.

Bis heute ist auch der **Begriff der Information** von zentraler Bedeutung, nicht nur im datenschutzrechtlichen Sinne. Der Mensch ist – auch ohne technische Hilfsmittel – grundsätzlich aufgrund seiner Sprachfähigkeiten in der Lage, große Mengen von Informationen aufzunehmen, weiterzugeben und zu speichern. Auch hat der Mensch seit langer Zeit Möglichkeiten gesucht und gefunden, Informationen über große Distanzen zu transportieren. Unterschiedliche Transportmittel wurden genutzt: Rauch- und Lichtzeichen, Brieftauben, Boten und Postdienstleister und seit der viktorianischen Zeit auch Tiefseekabel, die Mitte des 19. Jahrhunderts mit immensem Aufwand zwischen Europa und Nordamerika verlegt wurden. Das transatlantische Tiefseekabel konnte telegrafische Mitteilungen, also Morsecodes, in wenigen Stunden zwischen der „Alten und Neuen Welt“ übermitteln und somit ein neues Kommunikationszeitalter einläuten.

Bis heute ist das Transportmittel Seekabel das bedeutendste, da 99 Prozent des weltweiten Datenverkehrs darüber laufen. Es würde daher nicht wundern, wenn etwa die Beschädigungen von Untersee-Datenkabeln in der Ostsee Ende des Jahres 2024 Sabotageakte waren. Denn der Bedarf, Informationen auszutauschen, aber auch zu unterbinden oder Desinformationen zu streuen, ist scheinbar unbegrenzt.

Informationen, die in falsche Hände geraten oder schlicht falsch sind, stellen ein Risiko dar. Die Risiken können sich im Einzelfall für eine betroffene Person entfalten, aber auch für Unternehmen und Gesellschaften. Mit der Zunahme der Verbreitungstechniken und der fortschreitenden Digitalisierung nehmen diese Risiken weiter zu. Die Regulierung von Technik folgt deshalb seit jeher einem risikobasierten Ansatz: Zum einen müssen technische Maßnahmen ergriffen werden, um Risiken gering zu halten. Zum anderen werden organisatorische Vorgaben getroffen, die Risiken minimieren sollen. Bei den organisatorischen Maßnahmen spielt Sprache wiederum eine entscheidende Rolle: Die bereits erwähnten vielfältigen Sprachfähigkeiten des Menschen sind nicht nur ein Segen, sondern auch ein Risiko. Organisatorisch müssen daher verbindliche Verständigungen getroffen werden, was unter bestimmten Informationen zu verstehen und welche Bedeutung ihnen zuzumessen ist.

Der Anfang zur Schaffung derartiger organisatorischer Maßnahmen wurde gemacht und muss nun weiterwachsen: **Ein einheitliches Begriffsverständnis von bestimmten Informa-**

tionen muss übergreifend hergestellt und Informationen klassifiziert werden, damit in den zahlreichen technischen Systemen die Persönlichkeitsrechte von betroffenen Personen gewahrt bleiben und Informationen richtig, sicher und rechtmäßig verarbeitet werden.

Sprache ist Ausdruck und Träger von Kultur, aber zugleich auch ein Werkzeug. Gerade bei der Nutzung von Informationstechniken und Anwendungen Künstlicher Intelligenz lohnt der geschulte Einsatz eines sicheren und qualitativ hochwertigen Werkzeugs, um ein einheitliches Verständnis herbeizuführen und Schäden abzuwenden.

B. Rechtsgrundlagen und Zuständigkeiten des Rundfunkdatenschutzbeauftragten des NDR

Die einschlägigen Rechtsgrundlagen (§§ 43 bis 46 NDR Staatsvertrag und die Datenschutzgrundverordnung (DSGVO)) für den Auftrag und die Aufgaben des Rundfunkdatenschutzbeauftragten des NDR als Aufsichtsbehörde nach Art. 51 DSGVO blieben unverändert. Es gilt, die Einhaltung der Datenschutzvorschriften bei der **gesamten Tätigkeit des NDR und seiner Beteiligungsunternehmen** zu überwachen. Außerdem waren Beschwerden zu prüfen, die Personen einreichen können, wenn sie meinen, dass ein gegen den NDR gerichteter Anspruch auf Informationszugang zu Unrecht abgelehnt, nicht beachtet oder nur eine unzulängliche beantwortet wurde (§ 47 NDR Staatsvertrag).

C. Personalien

In der seit dem 25. Mai 2022 andauernden zweiten Amtszeit des Rundfunkdatenschutzbeauftragten des NDR hat es eine personelle Änderung hinsichtlich der Mitarbeiterin gegeben. Im Übrigen war und bleibt der Rundfunkdatenschutzbeauftragte des NDR weiterhin stellvertretender 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

Wie in den Berichten zuvor, folgt hier ein kurzer Überblick über wesentliche Entwicklungen auf dem Gebiet des Datenschutzes, soweit sie Relevanz für den öffentlich-rechtlichen Rundfunk haben.

I. EU-Kommission

Das Datenschutzrecht ist seit geraumer Zeit kein nationales Rechtsgebiet mehr, sondern vom Europarecht geprägt. Kleinteilige nationale Regelungen könnten dem europäischen und internationalen Datenverkehr kaum gerecht werden.

Die europäische Verordnung über Künstliche Intelligenz (KI-Verordnung) trat am 1. August 2024 in Kraft. Sie hat zum Ziel, einen einheitlichen Rahmen für den Einsatz von KI in den EU-Länder zu schaffen. Wie eingangs erwähnt, werden „Techniken“ nach ihren **Risikopotenzialen** reguliert. Dieser **risikobasierte Ansatz** sieht im Falle der KI-Verordnung wie folgt aus: Der Gesetzgeber differenziert zwischen Anwendungen Künstlicher Intelligenz in unterschiedlichen Risikoklassen und leitet daraus Folgerungen ab, und zwar für:

- **KI mit minimalem Risiko**: KI-Systeme dieser Klasse (z. B. Spamfilter, KI-gestützte Videospiele) unterliegen keinen besonderen Verpflichtungen, Unternehmen können aber freiwillig zusätzliche Verhaltenskodizes aufstellen.
- **besondere Transparenzverpflichtungen**: KI-Systeme wie Chatbots müssen ihre Nutzenden darauf hinweisen, dass sie mit Maschinen kommunizieren und durch KI erzeugte Inhalte müssen als solche gekennzeichnet werden.
- **KI mit hohem Risiko**: Hochriskante KI-Systeme (z. B. KI-basierte medizinische Software oder KI-Systeme für die Personaleinstellung) werden streng reguliert. Es müssen Risikominderungssysteme eingesetzt, die Nutzenden transparent informiert werden und eine menschliche Aufsicht gewährleistet sein.
- **KI mit unannehmbarem Risiko**: Diese KI-Systeme sind verboten, weil von ihnen eine klare Bedrohung für die Grundrechte der Menschen ausgeht (z. B. Bewertung des sozialen Verhaltens (Social Scoring)).

Die KI-Verordnung hat eine Reihe weiterer Regelungen, auf deren Umsetzung noch eingegangen wird, weil die Rundfunkdatenschutzkonferenz für den Einsatz von KI eine spezifische Empfehlung abgegeben hat.

II. Der Europäische Datenschutzausschuss (EDSA)

Der Europäische Datenschutzausschuss (EDSA) ist ein unabhängiges europäisches Gremium, in dem die nationalen Datenschutzbehörden des Europäischen Wirtschaftsraums und der Europäische Datenschutzbeauftragte (EDSB) Mitglieder sind. Aufgabe des EDSA ist, sicherzustellen, dass die Regelungen der DSGVO (und die Strafverfolgungsrichtlinie) einheitlich angewendet werden. Dazu fasst der EDSA verbindliche Entscheidungen.

Befasst hat sich der EDSA unter anderem mit dem **Trans-Atlantic Data Privacy Framework (DPF)**. Das DPF aus dem Jahr 2023 hält regulatorisch fest, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen dieses Abkommens aus der EU an US-Unternehmen übermittelt werden. „Angemessen" meint, dass die USA ein mit dem der Europäischen Union vergleichbares Datenschutzniveau vorweisen können. Dazu hatten die USA diverse Maßnahmen zu ergreifen.

Die Wirksamkeit des Abkommens sollte nach einem Jahr überprüft werden. Dies ist nun geschehen: Der EDSA kam zu dem Ergebnis, dass die Bemühungen der US-Behörden bislang hinreichend seien, das Abkommen mithin weiterhin Bestand haben könne. Allerdings sollen die Entwicklungen weiter im Blick behalten werden, da aufgrund des Politikwechsels in den USA Änderungen eintreten könnten.

Auch hat sich der EDSA einigen Grundsatzthemen angenommen, etwa den **Rechtsgrundlagen von Datenverarbeitungen** auf der Grundlage des sogenannten „berechtigten Interesses" (Art. 6 Abs. 1 lit. f) DSGVO) und Pflichten von Unternehmen bei der Beauftragung von Auftragsverarbeitern und Unterauftragsverarbeitern.

Zudem wurden Leitlinien erlassen, die sich mit der **Datenschutzrichtlinie für elektronische Kommunikation** (RL 2002/58/EG, ePrivacy-Richtlinie) befassen. Hier geht es um technische Belange, nämlich um die Speicherung und den Zugriff auf Informationen in

Endgeräten von Nutzenden (z. B. URL- und Pixel-Tracking, lokale Verarbeitungen, IP-basiertes Tracking).

III. Bundesgesetzgebung

Fast wäre es zu einem lange in Aussicht genommenen **Beschäftigtendatenschutzgesetz** gekommen. Mit Bearbeitungsstand vom 8.10.2024 wurde ein entsprechender Referentenentwurf des Bundesministeriums für Arbeit und Soziales und des Bundesministeriums des Innern und für Heimat vorgelegt. Der Bruch der Koalition hat das Vorhaben allerdings ausgebremst. Der Beschäftigtendatenschutz war in Deutschland seit jeher schwach ausgeprägt und zuletzt waren die wenigen Regelungen (§ 26 BDSG) durch die Rechtsprechung kritisch bewertet worden (EuGH, Entscheidung vom 30.03.2023, Rechtssache C-34/21).

IV. Rechtsprechung

Die Rechtsprechung war weiterhin äußerst aktiv. Besondere Aufmerksamkeit lag auf den Voraussetzungen für immateriellen Schadensersatz.

1. Immaterieller Schadensersatz

Unter welchen Voraussetzungen ein immaterieller Schaden vorliegt, der auch zu einem Schadensersatz führt, war lange unklar. Der Bundesgerichtshof hat sich in seinem Urteil (Az. VI ZR 10/24) zum sogenannten „Scraping-Komplex“ dazu nun grundsätzlich geäußert. Scraping bedeutet in diesem Zusammenhang das automatisierte Auslesen von Inhalten von Webseiten. Im Jahr 2021 hatten Unbekannte Daten von etwa 553 Millionen Nutzenden eines sozialen Netzwerks veröffentlicht. Diese waren in dem Netzwerk überwiegend frei zugänglich. Der BGH hat angenommen, dass ein **bloßer, vorübergehender Verlust der Kontrolle über personenbezogene Daten** ausreicht, um einen Anspruch auf den Ersatz eines immateriellen Schadens zu begründen. Eine besondere Beeinträchtigung durch die betroffenen Personen müsse nicht nachgewiesen werden. Ein Kontrollverlust – dieser muss tatsächlich gegeben sein – reiche aus, um einen immateriellen Schaden zu begründen. Angemessen sei ein Betrag in Höhe von 100 Euro.

Aber auch eine **Entschuldigung** kann einen angemessenen Ersatz eines immateriellen Schadens darstellen, so der EuGH (Urteil vom 04.10.2024, Rs. C-507/23). Gerade wenn keine Möglichkeit besteht, die Lage vor dem Schadenseintritt herzustellen, komme eine Entschuldigung in Betracht.

Eine Reihe von Entscheidungen sind zu dieser Thematik ergangen. Zu beachten ist dabei stets, dass die **Darlegungspflicht eines Schadens** der betroffenen Person obliegt. Nicht jeder Verstoß gegen datenschutzrechtliche Vorgaben begründet zugleich auch einen Schadensersatzanspruch. Ob ein immaterieller Schaden vorliegt, ist daher anhand der Umstände des jeweiligen Falles zu prüfen. Betroffene müssen mithin auf ihren Fall bezogenen darlegen, dass und aufgrund welcher Umstände sie einen immateriellen Schaden erlitten haben. Der EuGH hat dazu ausgeführt, dass zumindest die Befürchtung, einen Kontrollverlust erlitten zu haben nebst negativen Konsequenzen, nachzuweisen ist (EuGH, Urteil vom 20.06.2024, Rs. C-590/22).

Auskünfte über verarbeitete Daten einer Person (Art. 15 DSGVO) müssen z. B. innerhalb eines Monats erteilt werden. Bei verspätet erteilten Auskünften haben die Gerichte regelmäßig keinen Anspruch auf immateriellen Schadenersatz erkannt, weil nicht zu erkennen sei, ob und wie sich ein Kontrollverlust manifest haben könnte (so etwa das Bundessozialgericht, Urteil vom 24.09.2024, Az. B 7 AS 15/23 R; ArbG Hannover, Urteil vom 30.05.2024, Az. 2 Ca 325/23).

2. Widerruf einer Einwilligung in Ton- und Bildaufnahmen

Das OLG Koblenz hatte sich mit einer Sache zu befassen, die auch regelmäßig Gegenstand der hiesigen Beratungstätigkeit und Schulungen ist. Personen haben grundsätzlich eine Einwilligung zu erteilen, wenn von ihnen Bild- oder Tonaufnahmen veröffentlicht werden sollen. Nicht selten kommt es vor, dass die Einwilligungen widerrufen werden. Die Gründe werden oftmals nicht mitgeteilt. Das OLG Koblenz hat entschieden (Beschluss vom 31.07.2024, Az. 4 U 238/23), dass ein solcher Widerruf einer Einwilligung zur Veröffentlichung von Videoaufnahmen möglich ist und die Voraussetzungen des **Kunsturhebergesetzes** anzuwenden sind. Ein wirksamer Widerruf der Einwilligung bedarf danach aber besonderer Gründe: Das Persönlichkeitsrecht der betroffenen Person muss durch die Veröffentlichung schwerwiegend beeinträchtigt sein.

3. Zum Recht auf Auskunft über die Verarbeitung personenbezogener Daten

Hinsichtlich des Rechts auf Auskunft gemäß Art. 15 DSGVO sind zahlreiche Urteile ergangen, die sich insbesondere mit dem Umfang der Auskünfte befassen. Der Umfang einer Auskunft bezogen auf den Einzug der Rundfunkbeiträge ist spezialrechtlich ausgeformt in § 11 Absatz 8 Rundfunkbeitragsstaatsvertrag. Die entsprechend erteilten Auskünfte sind nicht nur Gegenstand von Beschwerden, sondern beschäftigen auch die Gerichte. Rechtskräftige obergerichtliche Entscheidungen dazu sind aber noch nicht ersichtlich.

Der einschlägige Erwägungsgrund 63 zu Art. 15 DSGVO lautet:

„Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. […] Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. […]“

Das OLG Frankfurt hat mit Beschluss vom 02.07.2024 (Az. 6 U 41/24) festgestellt, dass solche „Fernzugänge“ durch **Selbstbedienungstools** bereitgestellt werden können: „Die Bereitstellung eines angemessenen Fernzugangs über ein Self-Service-Tool wird daher als ausreichend angesehen, um den Anspruch auf Bereitstellung einer Kopie der personenbezogenen Daten gemäß Art. 15 Abs. 3 Satz 1 DSGVO zu erfüllen.“ Hierüber sollten Verantwortliche nachdenken – zumindest in Ergänzung anderer Möglichkeiten –, weil damit Nutzende in die Lage versetzt werden, sich jederzeit selbst einen Überblick über die ihre Person betreffenden Datenverarbeitungen zu verschaffen. **Der Beitragsservice bietet ein solches Tool bereits an**.

4. Beschäftigtendatenschutz

Nicht alles, was „öffentlich“ im Internet abrufbar ist, kann voraussetzungslos genutzt werden: Ein Arbeitgeber hatte durch eine Recherche mit einer Suchmaschine Kenntnis erlangt, dass ein Bewerber eine Vorstrafe hat. Die Speicherung dieser Information

ist eine Datenverarbeitung, über die eine **Informationspflicht gemäß Art. 14 DSGVO** besteht. Kommt das Unternehmen dieser Informationspflicht nicht nach und verwertet die Information im Bewerbungsverfahren, begründet dies einen Schadensersatz (LAG Düsseldorf, Urteil vom 10.04.2024, Az. 12 Sa 1007/23). Recherchen über Bewerber*innen und bereits beschäftigte Personen sind mithin nicht „ohne weiteres" möglich. Es ist – wie so oft – eine Frage des konkreten Einzelfalles. Denn Internetrecherchen aufgrund eines Bewerbungsverfahrens und sogar Nachfragen bei anderen Unternehmen können zur Wahrung berechtigter Interessen eines Unternehmens dann zulässig sein, wenn der begründete Verdacht besteht, dass „**AGG-Hopping**" betrieben wird (LAG Hamm, Urteil vom 05.12.2023, Az. 6 Sa 896/23). AGG-Hopper sind Personen, die sich nicht ernsthaft auf offene Stellen bewerben, sondern Entschädigungszahlungen wegen behaupteter Verstöße gegen das Diskriminierungsverbot erlangen möchten.

Aber auch beschäftigte Personen sind an datenschutzrechtliche Vorgaben gebunden, selbst wenn nicht jeder Verstoß gegen diese Vorschriften ein wichtiger Grund gemäß § 626 Abs. 1 BGB darstellt und somit eine fristlose Kündigung rechtfertigt. Wer aber beispielsweise im Beschäftigtenkontext **E-Mails mit sensiblen Daten des Arbeitgebers und anderer Dritter an seinen privaten E-Mail-Account** weiterleitet, kann fristlos gekündigt werden (OLG München, Urteil vom Urteil vom 31.07.2024, Az. 7 U 351/23 e).

5. EU-Kommission gegen EDSB

Nachdem der Europäische Datenschutzbeauftragte (EDSB) diverse Datenschutzverstöße bei der Nutzung von Microsoft-Anwendungen durch die EU-Kommission beanstandet hatte, verklagt diese nun den EDSB. Als Abhilfemaßnahme hatte der EDSB der EU-Kommission aufgegeben, dass mit Wirkung vom 9. Dezember 2024 alle Datenströme ausgesetzt werden, die sich aus der Nutzung der entsprechenden Anwendungen ergeben. Die EU-Kommission ist allerdings der Auffassung, bereits hinreichende Schutzmaßnahmen ergriffen zu haben und verklagt daher den EDSB vor dem Gericht der Europäischen Union. Microsoft hat sich der Klage angeschlossen. Der Ausgang dieses Verfahrens dürfte zukünftig viele Unternehmen betreffen.

E. Tätigkeiten des Rundfunkdatenschutzbeauftragten des NDR im Jahr 2024

Die Aufgaben einer Datenschutzaufsicht sind gesetzlich festgeschrieben, weshalb es eine gewisse Kontiunität in der Tätigkeit gibt. Die Schwerpunkte haben sich allerdings verlagert. Strukturell gab es im Jahr 2024 keine Änderungen, weil sich die etablierten Strukturen und Arbeitsteilungen bewährt haben.

I. Zusammenarbeit und Vernetzung

Diese Konferenzen und Arbeitskreise bestehen nach wie vor:

- Die **Rundfunkdatenschutzkonferenz** (RDSK): Das sind die als datenschutzrechtlichen Aufsichtsbehörden tätigen Personen im öffentlich-rechtlichen Rundfunk.
- Der **Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradios** (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.

Informationen und Veröffentlichungen dieser Gremien 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 RDSK ist der Zusammenschluss der Aufsichtsbehörden über den öffentlich-rechtlichen Rundfunk. Die bereits bestehenden Gemeinschaftsangebote und Gemeinschaftseinrichtungen und die auch gesetzlich forcierte Zusammenarbeit der Rundfunkanstalten spiegelt sich in der Tätigkeit der RDSK wider. Die Fülle der zu überwachenden Tätigkeiten macht eine Arbeitsteilung auch bei den Aufsichten notwendig. Wie dies geschieht, ist der Webseite der RDSK zu entnehmen:

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

Auch die Orientierungshilfen und Empfehlungen der RDSK sind dort zu finden.

a) Organisation der RDSK

Die RDSK hat vier Mitglieder, die auf der Grundlage einer „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten“ und einer „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten“ zusammenarbeiten und regelmäßig zweimal jährlich tagen.

b) Tätigkeitsschwerpunkte der RDSK

Die RDSK hat sich eingehend mit **Nutzungsmessungen** in Telemedienangeboten befasst und geprüft. Das Thema ist von dauerhafter Relevanz, weil nach Auffassung der RDSK Nutzungsmessungen (nur) dann ohne Einwilligungen der Nutzenden möglich sind, wenn dies anonymisiert passiert. Deshalb bildete die Prüfung der Einhaltung dieser Anforderungen einen Schwerpunkt.

Ein weiterer Schwerpunkt war der **Einsatz von Künstlicher Intelligenz**. Die RDSK hat dazu ein umfangreiches Papier erstellt und konkrete Handlungsvorgaben für einen datenschutzkonformen Einsatz von KI gegeben:

https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/orientierungshilfe-zum-datenschutzkonformen-einsatz-von-ki-im-oeffentlich-rechtlichen-rundfunk

Hier ein wesentlicher Auszug:

„Um einen Einsatz von KI rechtssicher zu ermöglichen, ist […] Folgendes zu beachten:

1. Redaktionelle Zwecke

- KI-Anwendungen (auch offene Systeme) können redaktionelles Arbeitsmittel und/oder Berichtsgegenstand sein. Für die Nutzung zu beiden Zwecken werden regelmäßig personenbezogene Daten von den Anwendungen verarbeitet (z. B. E-Mail-Adressen, aber auch Protokoll- und Nutzungsdaten, Benutzerinhalte und Kommunikationsinformationen (Namen)). Daher ist darauf zu achten, dass Beschäftigte möglichst wenig Daten preisgegeben – Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO).
- Bei Nutzung offener Systeme ist nach Möglichkeit die Nutzung der Daten für das Training der KI auszuschließen (z. B. in den Einstellungen der jeweiligen Anwendung).
- Die eingesetzten Systeme dürfen die Einhaltung des Datengeheimnisses nicht gefährden und den Grundsatz der Vertraulichkeit und Integrität zur Gewährleistung der Datensicherheit nicht verletzen. Die in die offenen KI-Anwendungen eingespeisten Inhalte dürfen daher nicht vertraulich sein. D. h.:
  - Vertrauliche (redaktionelle) Informationen und Redaktionsgeheimnisse dürfen nicht in offene KI-Anwendungen im Internet eingespeist werden.
  - Der Informantenschutz muss stets gewahrt bleiben.
- Beim Einsatz von KI sind die Programmgrundsätze zu wahren. Auch bei KI-generierten Programmangeboten gilt die journalistische Sorgfaltspflicht.
- Die Persönlichkeitsrechte betroffener Personen sind auch beim Einsatz von KI zu wahren.
- Kinder genießen besonderen Schutz. Dieser muss auch beim Einsatz von KI beachtet werden.
- Der Verantwortliche sollte prüfen, ob Angebote, die mithilfe von KI ganz oder teilweise erstellt werden, entsprechend gekennzeichnet werden.
- Die von KI-Anwendungen verarbeiteten Daten können urheberrechtlich geschützt sein. Die Vorgaben des Urheberrechts gelten auch beim Einsatz von KI.

2. Unternehmensinterne Zwecke

- Hinsichtlich des diesbezüglichen Einsatzes von KI ist zu beachten, dass interne, vertrauliche und streng vertrauliche Informationen nicht in offene KI-Systeme eingespeist werden dürfen.

- Daten aus einem Intranet, interner Schriftverkehr, Korrespondenzen mit Geschäftspartnern, Beschäftigtendaten (etwa Daten zu Einkommen, Bewerbungsunterlagen, Arbeitszeugnisse, Gesundheitsdaten, Daten für die interne Personalplanung) oder auch Geschäftsgeheimnisse (z. B. streng vertrauliche Revisionsberichte) können aufgrund der benannten Risiken nicht mit offenen KI-Systemen verarbeitet werden.
- Offene KI als Arbeitsmittel für unternehmensinterne Zwecke kann mithin nur für solche Informationen eingesetzt werden, die ohnehin öffentlich sind (dies sind z. B. öffentlich erreichbare Internetseiten, öffentlich zugängliche Verzeichnisse oder andere öffentlich zugängliche Quellen (Pressemitteilungen, frei zugängliche Medienangebote)).
- An eine automatisierte Anbindung bzw. voreingestellte technische Verknüpfung von bestimmten Tools mit anderen bereits eingesetzten Anwendungen (z. B. bei Microsoft-365-Produkten) sind besonders hohe Anforderungen zu stellen. Voreingestellte technische Verknüpfungen sollten grundsätzlich deaktiviert werden, um vor einer sonst ggf. automatisierten Implementierung eine sorgfältige Prüfung zu ermöglichen.
- Der Einsatz von geschlossenen KI-Anwendungen (z.B. On-Premise oder Private-Cloud) ist vorzugswürdig, weil solche Systeme nur für die Mitarbeitenden der Rundfunkanstalten zugänglich sind und keine Schnittstelle zum Internet haben. Die bei Anwendung eingegebenen oder entstehenden Daten werden vom Anbieter der KI damit nicht zum Training der KI verwendet."

Neben weiteren Hinweisen und Erläuterungen wird auch eine **Checkliste** zum datenschutzkonformen Einsatz von KI bereitgestellt.

Erforderlich waren zudem die Veröffentlichungen von „Grundlagen für die Verhängung von **Bußgeldern** gem. Art. 58 Abs. 2 lit. i) DSGVO" (bezüglich kommerzieller Tochterunternehmen) und zu „**Datenschutzfolgenabschätzungen** – Listen gemäß Art. 35 Abs. 4 und 5 DSGVO.

Alle Veröffentlichungen sind im Volltext zu finden unter https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen.

c) Vernetzung der RDSK mit anderen Medienaufsichten

Erstmals hat sich die RDSK auch nur mit Aufsichtsbehörden über private Medien ausgetauscht. Mit dem „Medienbeauftragten für den Datenschutz Bayerische Landeszentrale für neue Medien (BLM)“ und der „Beauftragten für Datenschutz der Landesanstalt für Medien NRW“ wurden Zuständigkeiten, Strukturen und Organisation der Aufsichtsbehörden erörtert. Weiterhin ging es um aktuelle datenschutzrechtliche Schwerpunktthemen im Medienbereich. Zudem wurden Perspektiven und Inhalte für weitere Zusammenkünfte ausgelotet.

d) Austausch mit der Datenschutzkonferenz

Zweimal jährlich treffen sich Mitglieder der **Datenschutzkonferenz** (DSK), also dem Gremium der Datenschutzaufsichtsbehörden des Bundes und der Länder, der RDSK und die datenschutzrechtlichen Aufsichtsbehörden der Kirchen und des privaten Rundfunks. Die Protokolle sind hier einsehbar:

https://www.datenschutzkonferenz-online.de/protokolle.html

Organisatorisch ging es unter anderem um die Art und Weise der Vernetzung miteinander. Inhaltlich gab es, neben zahlreichen anderen Themen, einen Austausch zu Künstlicher Intelligenz und der Rolle der Datenschutzaufsichten nach der KI-Verordnung. Dieses Thema wird noch intensiver zu erörtern sein, weil gemäß Art. 74 Abs. 8 KI-Verordnung die **Datenschutzaufsichtsbehörden auch die Marktüberwachungsbehörden** für bestimmte Bereiche sein sollen. Wie dies in der Praxis auszugestalten ist, bleibt noch zu klären.

e) Zukunft der RDSK

Eine Konferenz macht nur Sinn, wenn sich mehrere Personen austauschen (das Wort stammt aus dem Lateinischen und bedeutet „zusammentragen“, „vergleichen“). § 31j des Entwurfs der Rundfunkkommission für einen „Staatsvertrag zur Reform des öffentlich-rechtlichen Rundfunks (Reformstaatsvertrag) schafft die RDSK jedoch faktisch ab, da der Gesetzgeber nunmehr einen „gemeinsamen Rundfunkdatenschutzbeauftragten“ für die Landesrundfunkanstalten, das

ZDF und das Deutschlandradio etablieren möchte. Begründet wird dies wie folgt: „Im Sinne einer stärkeren Zusammenarbeit wird ein gemeinsamer Rundfunkbeauftragter für den Datenschutz vorgesehen. Schon heute haben bereits folgende Anstalten einen „gemeinsamen“ Rundfunkdatenschutzbeauftragten: BR, HR, MDR, RBB, SR, SWR, WDR, ZDF, DLR. Die Verfahren werden durch die einheitliche Regelung vereinfacht und einheitliche Maßgaben zur Datenschutzaufsicht geschaffen.“

Das Erreichen des gesetzgeberischen Ziels einer „stärkeren Zusammenarbeit“ dürfte durch die Ernennung nur einer Person kaum erreichbar sein, weil der Austausch mit anderen Aufsichten ja gerade entfiele. Es gäbe mithin keine Zusammenarbeit mehr. Ein Austausch der Mitglieder der RDSK mit der Datenschutzkonferenz der Länder und des Bundes wird bereits durchgeführt (s. o.) und ist nach Maßgabe des § 18 Abs. 1 S. 4 BDSG gesetzlich verankert: „Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.“ Dort können aber keine rundfunkspezifischen Themen erörtert werden, weil dies „andere“ Angelegenheiten darstellen, die die Länder und den Bund nicht betreffen.

Die RDSK hat mithin bereits auf der Grundlage von europarechtlichen Vorgaben (Artt. 60, 61 DSGVO) und aus eigenen Erwägungen eine funktionierende Zusammenarbeit etabliert und verständigt sich auf einheitliche Standards, wie den Veröffentlichungen der RDSK entnommen werden kann.

Kern der in Aussicht genommenen Reform ist eine stärkere Kosteneffizienz des öffentlichen-rechtlichen Rundfunks. Das dazu in Auftrag gegebene Sondergutachten der KEF hat jedoch keine Ersparnis im Bereich des Datenschutzes ermitteln können. Eine Steigerung der Kosteneffizienz ist grundsätzlich zu begrüßen. Daher war der gesetzgeberische Versuch unternommen worden, das sogenannte EfA-Prinzip zu etablieren: Einer für Alle. Eine ARD-Anstalt soll sich federführend um eine konkrete Aufgabe kümmern. Eine zentrale Datenschutzaufsicht und Marktüberwachungsbehörde würde jedoch aufgrund der gewachsenen Aufgaben eine Personalreduktion und Kostensenkung nicht erbringen können. Während die Aufsichtsbehörden der Länder und des Bundes wieder-

holt auf ihren erhöhten Personalbedarf hingewiesen haben, sollen die entsprechenden Aufsichtsbehörden für den öffentlich-rechtlichen Rundfunk zusammengelegt werden. Die Datenschutzkonferenz der Länder und des Bundes (DSK) arbeitet seit Jahren daran, datenschutzrechtliche Standards zu vereinheitlichen und durchzusetzen. Diese Aufgabe bezüglich des Rundfunks lediglich einer Behörde zu übertragen, würde einen **Entzug an Personal, Knowhow und Austauschplattform** bedeuten, aber insgesamt nicht zu einer personellen Reduktion führen.

An dieser Stelle sei daher erwähnt, dass die Anforderungen an die Tätigkeiten der Aufsichtsbehörden bereits in den vergangenen Jahren stetig gestiegen sind, etwa durch

- fortschreitende Regulierungen,
- umzusetzende Gerichtsentscheidungen,
- weitere Aufgaben hinsichtlich der Informationsfreiheit und
- technische Fortschritte, insbesondere KI.

Die Reform des Medienstaatsvertrages sieht nun an vielen Stellen vor, die Angebote des öffentlich-rechtlichen Rundfunks zu vernetzen und den Dialog mit dem Publikum zu intensivieren. So sollen die Möglichkeiten der Partizipation und Interaktion gestärkt (§ 26 Abs. 3 E-MedienStV), technische Plattformen mit Publikumsdialog geschaffen (§ 36 VI E-MedienStV) und fremde Portale vermehrt genutzt werden (§ 30 IV E-MedienStV). Zugleich tragen die Anstalten dabei eine „besondere Verantwortung“ bei der Verarbeitung der Nutzerdaten (§ 31i E-MedienStV) und nicht zuletzt wird der Einsatz von KI (§ 31m E-MedienStV) normiert. All dies bedeutet auch einen **Zuwachs an datenschutzrechtlichen Befassungen,** weil die Verarbeitung von personenbezogenen Daten zunimmt und nicht zuletzt auch mit einem erhöhten Beschwerdeaufkommen zu rechnen ist.

Auch die Einzelheiten der entsprechenden Vorschriften geben Zweifel auf, so etwa das komplizierte Ernennungsverfahren durch alle Rundfunkräte (bzw. den Fernseh- und Hörfunkrat). Weiterhin ist der Rundfunkdatenschutzbeauftragte des NDR beispielsweise auch **Beauftragter für die Informationsfreiheit** (s. o.

unter B.: „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 Abs. 11 NDR Staatsvertrag). Dies entspricht den Regelungen der Bundesländer, in denen regelmäßig die Landesdatenschutzbeauftragten zugleich die Beauftragten für die Informationsfreiheit sind. Eine Regelung für diese Zuständigkeit findet sich im Entwurf des Medienstaatsvertrags nicht.

§ 31l E-Medien-StV bestimmt, dass der gemeinsame Rundfunkdatenschutzbeauftragte die „gesamte Tätigkeit“ der beaufsichtigten Anstalten überwacht. Bisher gibt es für einige Anstalten eine geteilte Aufsicht, mithin eine Zuständigkeit eines Landesdatenschutzbeauftragten und einer spezifischen Rundfunkaufsicht (z. B. für den Hessischen Rundfunk). Mit der Regelung des § 31l E-Medien-StV entfielen die **Zuständigkeiten der Länder**. Dies ist grundsätzlich aufgrund von schwierigen Abgrenzungen zu begrüßen, führt aber zu einer Erhöhung des Arbeitsaufkommens des Rundfunkdatenschutzbeauftragten.

Alternativen wären denkbar: So ist in einem Entwurf zur Novellierung des Bundesdatenschutzgesetzes vorgesehen, die Datenschutzkonferenz der Länder und des Bundes zu „institutionalisieren“. Der Koalitionsvertrag (Zeilen 465 ff.) sieht vor: „Zur besseren Durchsetzung und Kohärenz des Datenschutzes […] institutionalisieren [wir] die Datenschutzkonferenz im Bundesdatenschutzgesetz (BDSG) und wollen ihr rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen.“

Als Pendant dazu könnte der Gesetzgeber des Medienstaatsvertrages die **RDSK entsprechend institutionalisieren** und dies in dem Staatsvertrag festschreiben. Dies würde das in Aussicht genommene Ziel der stärkeren Zusammenarbeit fördern.

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 unter anderem mit diesen Themen befasst:

- Auftragsverarbeitungen
- Aufzeichnungen von Videokonferenzen
- Joint-Controller-Vereinbarung ARD
- Anwendungen von KI aus datenschutzrechtlicher Sicht
- Hinweisgeberschutzgesetz – Informationspflichten
- DSGVO-konforme Vergabe/Beschaffung
- Kooperationen der Rundfunkanstalten im Programmbereich
- SAP-Harmonisierung
- Schutzbedarfsfeststellungen
- Ausschreibung der Festnetztelefonie
- ARD-Rahmenvertrag für Onlinebefragungen der Medienforschung

Die 97. Sitzung des AKDSB fand Ende November 2024 statt. Der Arbeitskreis, der regelmäßig zweimal im Jahr tagt, besteht also seit fast 50 Jahren. Daher ging es auch um die Rolle und Aufgaben des AKDSB, damit in den zahlreichen Vorhaben und (neuen) Gruppierungen der ARD weiterhin eine feste Verankerung und Beachtung datenschutzrechtlicher Anliegen gewährleistet ist. Der AKDSB hat daher verabredet, zukünftig präsenter in den Anstalten aufzutreten, Veröffentlichungen zu aktuellen Themen bereitzustellen und Aufgaben und Strukturen transparenter zu erläutern.

II. Tätigkeitsschwerpunkte bezüglich Datenverarbeitungen im NDR

„Der Schutz des Persönlichkeitsrechts: An erster Stelle nennt das Gesetz [...] die Aufgabe des Datenschutzbeauftragten, darüber zu wachen, daß die Angaben der Bürger und die über die einzelnen Bürger vorhandenen Unterlagen bei der maschinellen Datenverarbeitung durch die Behörden und Stellen der öffentlichen Verwaltung des Landes vertraulich behandelt werden.“ So formulierte der Hessische Datenschutzbeauftragte in seinem ersten Bericht aus dem Jahr 1972 seine vornehmliche Aufgabe. Der

Kern der Aufgaben ist damit bis dato zutreffend beschrieben, auch wenn die einzelnen Aufgaben in Art. 57 DSGVO ausdifferenzierter festgelegt wurden:

- die Anwendung dieser Verordnung [DSGVO] **überwachen und durchsetzen**
- die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung **sensibilisieren** und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder
- im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung **beraten**
- die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren
- auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten **zusammenarbeiten**
- sich mit **Beschwerden** einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist
- mit **anderen Aufsichtsbehörden zusammenarbeiten**, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten
- **Untersuchungen über die Anwendung dieser Verordnung durchführen**, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde
- **maßgebliche Entwicklungen verfolgen**, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken

Die Auflistung der Aufgaben gemäß Art. 57 DSGVO, die hier nur auszugsweise abgebildet ist, reicht von lit. a) bis v) und kennt daher **23 Aufgabenzuschreibungen**. Eine

Reihe von Aufgaben waren auch im Berichtsjahr zu erledigen. Die Schwerpunkte werden im Folgenden dargestellt. Sie sind – wie in den Berichten zuvor – gegliedert nach den Themen

- Programmerstellung und -verbreitung,
- Rundfunkbeitragseinzug,
- Beschäftigtendatenschutz,
- Organisations- und Strukturprojekte.

1. Zur Umsetzung der DSGVO

Die Errichtung einer Rechtsordnung ist immer ein Beginn und nie ein Ende. Die Regelungen müssen eingeübt, gelebt und überwacht werden. Neue Vorhaben und Prozesse müssen nach Maßgabe der Vorgaben etabliert werden. Aufsicht und Beratung ist somit eine fortwährende Aufgabe. Wie die Aufgaben wahrgenommen werden, liegt grundsätzlich im **Ermessensspielraum der Aufsichtsbehörde**. In seinem Urteil vom 26. September 2024 (Az. C-768/21) hat der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsersuchens entschieden, dass Aufsichtsbehörden im Falle der Feststellung einer Datenschutzverletzung **nicht zwingend verpflichtet sind, eine Abhilfemaßnahme zu ergreifen**, sofern ein solches Einschreiten nicht geeignet, erforderlich oder verhältnismäßig ist. Insbesondere wenn der für die Verarbeitung Verantwortliche umgehend die erforderlichen Maßnahmen ergreift und damit einer Wiederholung der Verletzung entgegentritt, kann von Abhilfemaßnahmen abgesehen werden. Dies schafft einerseits eine gewisse Flexibilität in der Aufsichtspraxis, andererseits nimmt es Befürchtungen seitens des Verantwortlichen, selbst auf Mängel hinzuweisen und um Beratung zu bitten.

2. Programm und Programmverbreitung

Hinsichtlich des Programms und seiner digitalen Verbreitung gab es aus datenschutzrechtlicher Perspektive keine wesentlichen Neuerungen. Die Anfragen und Themen verliefen in gewohnten Bahnen.

a) Datenschutzerklärungen und Informationspflichten

Besucher*innen hinterlassen Spuren. Dies gilt auch für die, die die digitalen Angebote des NDR und der ARD aufsuchen. Es werden bei dem Besuch einer Interseite zumindest IP-Adressen verarbeitet. Dies löst gemäß Art. 13 DSGVO Informationspflichten aus, die der NDR für die von ihm verantworteten Telemedienangebote in den jeweiligen Datenschutzerklärungen erfüllt. Erforderliche Anpassungen und Ergänzungen wurden erörtert, so etwa hinsichtlich des sogenannten **ARD-Kontos**: Die Landesrundfunkanstalten sind gemeinsam für die Datenverarbeitung im Rahmen des ARD-Kontos verantwortlich und haben dazu Art. 26 DSGVO eine Vereinbarung zur gemeinsamen Verantwortlichkeit abgeschlossen. Dies ist erforderlich, um Transparenz über die datenschutzrechtlichen Verantwortlichkeiten und Pflichten herzustellen.

b) Anfragen zu den Angeboten und Datenschutzerklärungen des NDR

Hierzu ist festzuhalten, dass die Ausführungen aus dem Tätigkeitsbericht für das Jahr 2023 nahezu unverändert auch für das Jahr 2024 gelten. Etwa 20 Zuschriften gab es wegen

- Nachfragen zu den Datenschutzbestimmungen der Telemedienangebote,
- der Nutzungsmessungen ohne Einwilligungserfordernis,
- der Verwendung einzelner Cookies,
- technischer Funktionalitäten und Serverdiensten,
- Datenverarbeitungen auf Drittplattformen,
- redaktionellen Inhalten, in denen Personen identifizierbar zu sehen waren,
- Lösch- bzw. Unterlassungs- und Anonymisierungsbegehren und
- Anforderungen an Personalisierungen.

Solange – und das war das Ergebnis der oben erwähnten Untersuchung der RDSK – die eingesetzten Messmethoden der Rundfunkanstalten nur mit anonymisierten Daten arbeiten, bedarf es keiner Einwilligungen und daher auch keiner Cookie-Banner für die Telemedienmedienangebote. Zwecks Vermeidung von Wiederholungen der einschlägigen ausführlichen Erläuterungen aus

dem Bericht des Vorjahres sei an dieser Stelle auf die aktualisierten „Empfehlungen zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten“ hingewiesen, die dieses Thema umfangreich beleuchten:

https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/empfehlungen-zum-einsatz-von-cookies-in-online-angeboten-der-rundfunkanstalten

Dort wird dies empfohlen:

„Spezifische Aufgabe des öffentlich-rechtlichen Rundfunks erklären:
Zurecht erwarten die Nutzer vom öffentlich-rechtlichen Rundfunk einen besonders hohen Datenschutzstandard. Da im allgemeinen gerade Cookies, die das Nutzungsverhalten erfassen und auswerten, nur mit ausdrücklicher Einwilligung der betroffenen Person eingesetzt werden dürfen, entsteht **erhöhter Aufklärungs- und Beratungsbedarf, wenn die Rundfunkanstalten weiterhin für einzelne Cookies keine Einwilligung einholen**. Sie sollten daher ihre Datenschutzerklärungen bzw. Cookie-Hinweise besonders sorgfältig und verständlich formulieren. Allgemeinplätze wie etwa das Bestreben, mithilfe eines Cookies „den Nutzern ein bestmögliches Angebot zur Verfügung zu stellen“, werden dem nicht gerecht. Insbesondere sollten die Rundfunkanstalten daher die spezifische Aufgabe und Funktion des öffentlich-rechtlichen Rundfunks erläutern und die sich daraus ergebende Rechtsgrundlage für den Einsatz des betreffenden Cookies nennen.
Opt-Out ggf. ermöglichen:
Die Rundfunkanstalten können es den Nutzern ihrer Telemedienangebote ermöglichen, die Datenverarbeitung zur Nutzungsmessung zu unterbinden (Opt-Out), und auf diese Möglichkeit in ihrer Datenschutzerklärung hinweisen.“

Manche Zuschriften thematisierten Sendungen, in denen (andere) Personen kenntlich zu sehen waren und sorgten sich um die **Wahrung der Persönlichkeitsrechte**. Die DSGVO ist auf Abbildungen von Personen anwendbar, da (bewegte) Bilder eine Person regelmäßig identifizierbar machen. Auch wenn die einschlägige Entscheidung des BGH schon vier Jahre alt ist, löst dies im-

mer wieder Nachfragen aus. Es gilt: **Das Kunsturhebergesetz findet im journalistischen Bereich weiterhin Anwendung** (BGH, Urteil vom 7. Juli 2020 (Az.: VI ZR 246/19), auch wenn die maßgebliche Feststellung des Gerichts etwas kompliziert klingt: „Der Anwendbarkeit der §§ 22, 23 KUG steht im hier betroffenen journalistischen Bereich die zwischenzeitlich eingetretene Geltung der [Datenschutzgrund-] Verordnung [...] schon deshalb nicht entgegen, weil die Länder 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 ausgenommen haben [...] 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."

Ein Recht auf Vergessenwerden, in Art. 17 DSGVO als Recht auf Löschung bezeichnet, kommt daher unter Umständen in Betracht, unterliegt aber besonderen Anforderungen (s. o. OLG Koblenz, Beschluss vom 31.07.2024, Az. 4 U 238/23).

c) Anfragen von Redaktionen

Auch diesbezüglich gilt, dass Inhalte und Umfang der Tätigkeit des Vorjahres entsprachen. Beraten wurde beispielsweise bezüglich

- der Beschaffung von Recherchetools,
- Anforderungen an Datenverarbeitungen von Nutzenden,
- Datenübermittlungen für Akkreditierungszwecke und zur Sicherheitsüberprüfung (Olympische Spiele in Paris, Hamburger Woche der Pressefreiheit, „Politik vor Ort"),
- Datenschutzfragen zum ESC,
- Datenschutz und Produzentenvereinbarungen,
- Anmeldungen und Registrierungen,
- Datenschutz bei Gewinnspielen,
- des Aussendens von Newslettern,
- Anforderungen an Community-Management-Systeme,
- des Bezugs von Newslettern,

- Datenschutzhinweisen und weitere Anforderungen zu #NDRfragt (#NDRfragt ist eine Umfrage- und Dialogplattform des NDR),
- Hinweisen und Erklärungen für Kandidat*innen in Sendungen des NDR.

Hinzugekommen ist allerdings eine Vielzahl von Anfragen, die sich mit dem Einsatz von Künstlicher Intelligenz befassten. So wurde beispielsweise (kurzzeitig) in Aussicht genommen, Texte von Posts der Nutzenden in den eigenen Social-Media-Präsenzen für ein KI-Training zu sammeln und auszuwerten.

Auch Meta hatte ein ähnliches Ansinnen verfolgt und beabsichtigte, Daten der Nutzenden (für andere, neue Zwecke) zu verarbeiten, um damit sein Angebot zu verbessern und der Kundschaft ein besseres Angebot zur Verfügung zu stellen. Dieses Vorhaben wurde zunächst gestoppt, da Meta nach entsprechender Kritik auf das Vorhaben verzichtete. Das Unternehmen meinte, das Verwenden der Nutzerdaten zum Trainieren der KI sei zulässig, da es ein berechtigtes Interesse aus Art. 6 Abs 1 lit. f) DSGVO an der Verarbeitung habe. Daher sei das Einholen von Einwilligungen der Nutzenden nicht erforderlich. Dagegen wurden jedoch Bedenken laut, weil – auch nach den eigenen Angaben von Meta – keine Möglichkeit bestehe, zwischen personenbezogenen Daten und sensiblen Daten im Sinne des Art. 9 DSGVO zu unterscheiden. Letztere können nur unter bestimmten strengen Voraussetzungen verarbeitet werden. Ein sogenanntes berechtigtes Interesse reicht dafür nicht aus.

Die Nutzung auch öffentlicher Daten für eigene Zwecke (z. B. einer Rundfunkanstalt) muss mithin ebenfalls auf einer Rechtsgrundlage erfolgen. Die Verbesserung eines Angebots (oder die Erhöhung der Reichweite von betriebenen Seiten wie z. B. Fanpages etc.) kann nicht stets auf der Grundlage des berechtigten Interesses vorgenommen werden. Auch hilft insoweit nicht das Medienprivileg, weil dieses zwar Ausnahmen von datenschutzrechtlichen Vorgaben gewährt, nicht aber die Erforderlichkeit einer Rechtsgrundlage entfallen lässt. Es war daher festzuhalten, dass eine Rechtsgrundlage nicht erkennbar ist und auch die Öffentlichkeit der Posts nicht zugleich eine Einwilligung zur weiteren Verarbeitung durch Dritte darstellt.

3. Rundfunkteilnehmerdatenschutz

Schwerpunkte beim Rundfunkteilnehmerdatenschutz bildeten Anfragen und Beschwerden. Eine Reihe von Beschwerden wurde insbesondere zu Beginn des Jahres eingereicht. Benutzt wurde dazu ein im Internet veröffentlichter Vordruck, in dem standardisierte Behauptungen aufgestellt wurden, die regelmäßig in den geprüften Einzelfällen nicht zutrafen. So wurde etwa vorgetragen, Daten seien an bestimmte Stellen zu Unrecht weitergegeben worden oder der Beitragsservice dürfe bestimmte Verarbeitungstätigkeiten nicht vornehmen. Die Motivation dieser Beschwerden ist schwer zu ermitteln. Teilweilweise dürften Personen auf derartige Musterschreiben hereingefallen sein. In anderen Fällen dürfte es sich um den Versuch gehandelt haben, betriebliche Abläufe zu stören. Das Recht, eine Beschwerde zu erheben, steht zwar allen zu. Der überwiegend falsche Tatsachenvortrag in den Beschwerdeschreiben lässt jedoch an der Ernsthaftigkeit einiger Anliegen zweifeln. Die Beschwerden waren daher regelmäßig auch nicht erfolgreich.

Soweit an den Befugnissen des Beitragsservices gezweifelt wurde, lag dies an der mangelnden Kenntnis (oder bewussten Ignoranz) der einschlägigen Rechtsgrundlagen. Der NDR darf ganz oder teilweise die Abwicklung des Einzugs der Rundfunkbeiträge dem Beitragsservice übertragen. Geregelt ist dies in § 10 Absatz 7 Rundfunkbeitragsstaatsvertrag (RBStV):

„Jede Landesrundfunkanstalt nimmt die ihr nach diesem Staatsvertrag zugewiesenen Aufgaben und die damit verbundenen Rechte und Pflichten ganz oder teilweise durch die im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle der öffentlich-rechtlichen Landesrundfunkanstalten selbst wahr. Die Landesrundfunkanstalt ist ermächtigt, einzelne Tätigkeiten bei der Durchführung des Beitragseinzugs und der Ermittlung von Beitragsschuldnern auf Dritte zu übertragen und das Nähere durch die Satzung nach § 9 Abs. 2 zu regeln."

Der Beitragsservice ist mithin kein (privatwirtschaftlich organisierter) Dritter, sondern ein Teil (auch) des NDR. Die Regelungen des RBStV sind auch (verfassungs-) rechtlich nicht zu beanstanden. Dies hat das Bundesverfassungsgericht entschie-

den (BVerfG, Urteil des Ersten Senats vom 18. Juli 2018, - 1 BvR 1675/16 -, Rn. 1-157).

Auch der Erhalt von personenbezogenen Daten zur Ermittlung einer Beitragspflicht verstößt nicht gegen datenschutzrechtliche Bestimmungen, da er auf einer Gesetzesgrundlage beruht (Art. 6 Absatz 1 Satz 1 lit. c) DSGVO). Auf die Einwilligung der betroffenen Person kommt es daher nicht an. Die einschlägige Rechtsgrundlage findet sich in § 11 Absatz 4 RBStV. Danach verarbeitet die zuständige Landesrundfunkanstalt für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht besteht, personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis der betroffenen Person. Öffentliche Stellen sind insbesondere Meldebehörden.

Weiterhin ist die Weitergabe von Daten an Dritte gestattet, wenn Forderungen im Wege der Vollstreckung durchgesetzt werden sollen. Eine Landesrundfunkanstalt ist nur nicht berechtigt, für Zwecke der Beitragserhebung sowie zur Feststellung des Bestehens einer Beitragspflicht Daten zu erheben. Sie ist zudem befugt, Ansprüche im Verwaltungszwangsverfahren durchzusetzen. Die Rechtsgrundlage ist § 10 Absatz 6 RBStV.

Auf diese und weitere Fragen war u. a. in den Beschwerden einzugehen. **Im Jahr 2023 waren es rund 30 Beschwerden, im Berichtsjahr fast doppelt so viele**.

Im Jahr 2023 gab es beim Beitragsservice in Köln 1622 Auskunftsersuchen, die den NDR betrafen. **Im aktuellen Berichtsjahr hat der Beitragsservice insgesamt 25.925 Datenauskünfte versandt, davon 4.533 für den NDR**. Von diesen wurden wiederum 3.050 Stück auf elektronischem Weg über das Online-Portal beantragt. In 40 zusätzlichen Fällen wurde mitgeteilt, dass keine Daten gespeichert sind (Negativauskunft). Die Anzahl hat sich damit stark erhöht.

Beim NDR in Hamburg sind 17 Auskunftsanfragen eingegangen. Davon betrafen 2 Ersuchen ausschließlich den Beitragseinzug durch den NDR. Insoweit hat sich die Anzahl etwas verringert beziehungsweise auf den Beitragsservice verlagert.

4. Beschäftigtendatenschutz

Unter diesem Punkt geht es zum einen um Daten, die von Beschäftigten zur Abwicklung des Arbeitsverhältnisses verarbeitet werden. Dies meint der Begriff Beschäftigtendatenschutz. Zum anderen wird an dieser Stelle aber auch über Maßnahmen berichtet, die der NDR ergreift, um Beschäftigte im Datenschutz „fit" zu machen. Auch in diesem Sinne hat der Beschäftigtendatenschutz eine bedeutende Rolle.

a) Schulungen

Im Tarifvertrag über hybride Arbeit ist festgehalten, dass Beschäftigte, die hybrid („mobil") arbeiten, einen entsprechenden **Führerschein** absolvieren müssen (https://www.ndr.de/der_ndr/unternehmen/hybridearbeit100.pdf). Dazu gehört, dass jährlich wiederkehrend auch eine Schulung im Datenschutz durchzuführen ist. Dies gilt allerdings auch für Personen, die nicht hybrid arbeiten können oder wollen. Eine entsprechende Vereinbarung war mit dem NDR getroffen worden. Es hat sich jedoch leider herausgestellt, dass das nicht in allen Bereichen des NDR bekannt war. Abhilfe schaffen wird ein Tool, in dem zukünftig Pflichtschulungen dokumentiert werden. Dieses wird auch die zuständigen Personen an diese Pflicht erinnern.

Die Schulungen werden mit einem elektronischen Tool durchgeführt. Lediglich bestimmte Personengruppen sollen daher künftig, wie in diesem Jahr auch, persönlich geschult werden. Dazu gehören die neuen **Auszubildenden und Volontär*innen**. An dieser Stelle sei lobend erwähnt, dass einige Auszubildende angaben, ehrenamtlich als Datenschutzbeauftragte in Vereinen tätig (gewesen) zu sein. Dies zeigt, wie gut die Regelungen der DSGVO in der Praxis angekommen sind und wie gewachsen die Sensibilität für dieses Thema mittlerweile ist.

Mit den online-Schulungen für alle Beschäftigten entfallen allerdings keine persönlichen Schulungen durch den Rundfunkdatenschutzbeauftragen. Die entsprechenden Termine werden aber konfektioniert auf die einzelnen Bereiche zugeschnitten und sind deshalb ertragreicher und dialogisch angelegt.

Durchgeführt wurden Termine u. a. mit technischen Bereichen, der Medienforschung, der Personalabteilung, dem Gremienbüro, Social Media, Strategie und Innovation.

Auf Tätigkeiten in Bezug auf die Einführung Künstlicher Intelligenz wird noch eingegangen. An dieser Stelle sei nur bereits erwähnt, dass die Erarbeitung eines **KI-Führerscheins** begleitet wurde, der ebenfalls künftig verpflichtend sein wird. Denn die KI-Verordnung tritt stufenweise in Kraft und alle Arbeitgeber, deren Beschäftigte KI anwenden, müssen sicherstellen, dass bis zum 2. Februar 2025 (Art. 113 KI-VO) entsprechende KI-Schulungen durchgeführt werden. Der Inhalt der Schulungen wird in Art. 4 KI-VO umrissen:

„Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind."

Der entsprechende Erwägungsgrund der Verordnung lautet:

„Um den größtmöglichen Nutzen aus KI-Systemen zu ziehen und gleichzeitig die Grundrechte, Gesundheit und Sicherheit zu wahren und eine demokratische Kontrolle zu ermöglichen, sollte die KI Kompetenz Anbieter, Betreiber und betroffene Personen mit den notwendigen Konzepten ausstatten, um fundierte Entscheidungen über KI-Systeme zu treffen. Diese Konzepte können in Bezug auf den jeweiligen Kontext unterschiedlich sein und das Verstehen der korrekten Anwendung technischer Elemente in der Entwicklungsphase des KI-Systems, der bei seiner Verwendung anzuwendenden Maßnahmen und der geeigneten Auslegung der Ausgaben des KI-Systems umfassen sowie – im Falle betroffener Personen – das nötige Wissen, um zu verstehen, wie sich mithilfe von KI getroffene Entscheidungen auf sie auswirken werden. Im Zusammenhang mit der Anwendung dieser Verordnung sollte die KI-Kompetenz

allen einschlägigen Akteuren der KI-Wertschöpfungskette die Kenntnisse vermitteln, die erforderlich sind, um die angemessene Einhaltung und die ordnungsgemäße Durchsetzung der Verordnung sicherzustellen. […]“

Zwecks Einhaltung dieser Anforderungen wurde darauf hingewiesen, dass

- Beschäftigte, die KI anwenden, verpflichtend bis zum o. g. Datum eine KI-Schulung absolvieren sollten, wobei der Führerschein das Mittel der Wahl sein kann,
- der NDR die Durchführung der Schulung dokumentieren sollte, um seine Rechenschaftspflicht zu erfüllen.

b) Speicherfristen

Die Speicherfristen von personenbezogenen Daten haben sich nach gesetzlichen Fristen und dem Prinzip der Speicherbegrenzung des Art. 5 Abs. 1 lit. e) DSGVO zu richten. Insbesondere hinsichtlich Logdateien ist dieses Erfordernis immer wieder aus Sicherheitsgründen zu aktualisieren.

Nach einer NDR-internen Vorschrift gilt, dass personenbezogene Protokolldaten regelmäßig nach einer Woche zu löschen oder zu anonymisieren sind. Da weltweit Institutionen und Unternehmen durch zielgerichtete Cyberangriffe bedroht werden, muss angemessen und wirkungsvoll auf diese Art der Bedrohung reagiert werden können. Dies erfordert die Speicherung von Protokolldaten ausgewählter Systeme über einen längeren Zeitraum. Darüber hinaus ist der NDR verpflichtet, hochverfügbare und sichere Systeme bereitzustellen. Dazu müssen geeignete technische und organisatorische Maßnahmen ergriffen werden, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherstellen. Einige spezialrechtliche Anforderungen führen daher zu dem Bedarf, Löschfristen zu verlängern. Im Sinne der Datensicherheit gemäß Art. 5 Abs. 1 lit. f) DSGVO sind daher entsprechende Maßnahmen geboten, die erörtert und beraten wurden.

c) Harmonisierung von SAP-Systemen in der ARD

Dieses Projekt wurde formal Ende des Jahres 2024 abgeschlossen. Die Datenschutzbeauftragten der beteiligten Anstalten haben gemeinsam das Projekt beraten und einzelne Aspekte bewertet. In den Entwicklungs- und Testphasen gab es zahlreiche Hinweise, etwa zum Nutzungs-, Rollen- und Berechtigungsmanagement, und es wurde auf Mängel und Schwachstellen hingewiesen und Empfehlungen und Anweisungen zur Behandlung dieser gegeben. Auch nach der Inbetriebnahme der Systeme dürfte eine permanente Bearbeitung und ein kontinuierliches Monitoring erforderlich bleiben, um gemäß dem risikobasierten Ansatz der DSGVO die Datenverarbeitung nach den gesetzlichen Vorgaben vorzunehmen.

d) Desk-Sharing, Zeiterfassung, Umzüge

Auch diese genannten Themen waren Gegenstand der Tätigkeit im Jahr 2024. Die zukünftige Erfassung von Arbeitszeiten im gesamten NDR und das Buchen eines Arbeitsplatzes waren zu beraten. Denn die Arbeitssituationen vor Ort müssen auf die jeweiligen Anforderungen abgestimmt werden. Die Zuteilung von Räumlichkeiten und damit auch das Desk-Sharing haben Grenzen. In bestimmten Bereichen gelten besondere Anforderungen, etwa an spezielle Räumlichkeiten, so dass eine vertrauliche Kommunikation möglich ist. Gegebenenfalls ist ein entsprechendes Umfeld zu schaffen (z. B. mittels Telefonkabinen, Telefonräumen).

5. Künstliche Intelligenz

Der NDR hat begonnen, KI für unterschiedliche Geschäftszwecke zu erproben. Aus datenschutzrechtlicher Perspektive wurde der Prozess begleitet. Nach Maßgabe der bereits genannten Orientierungshilfe zum datenschutzkonformen Einsatz von KI im öffentlich-rechtlichen Rundfunk der RDSK war darauf zu achten, dass KI-Anwendungen auf der Grundlage eines geordneten Verfahrens eingeführt und nach abgestimmten Regeln erprobt werden, um etwaige Risiken von betroffenen Personen und Schäden für das einsetzende Unternehmen zu vermeiden.

Eine Reihe von Anwendungen kann kostenfrei über das offene Internet erreicht werden, gleichwohl ist die Nutzung nicht risikofrei. Im Gegenteil: Die kostenfreie Nutzung ergibt sich daraus, dass der KI-Anbieter die eingegebenen Informationen für sich und andere Unternehmen nutzt. Die eingegebenen Daten werden also häufig für kommerzielle Zwecke Dritter verwendet und unwiederbringlich veröffentlicht. Daher muss Klarheit bestehen, welche Datenverarbeitungen eine KI vornimmt, zu welchem Zweck und auf welcher Rechtsgrundlage der Einsatz erfolgen soll.

Entgegen einer weit verbreiteten Vorstellung erfordert der Einsatz von KI fast stets die Verarbeitung von personenbezogenen (Beschäftigten-) Daten. So etwa bei der Registrierung/Anmeldung zur Nutzung eines Tools. Auch gehören sensible Daten, wie etwa Gesundheitsdaten, Informationen über Herkunft, Ethnie, religiöse und weltanschauliche Überzeugungen sowie weitere höchstpersönliche und intime Informationen nicht in KI-Anwendungen. Gleiches gilt für unternehmensinterne Information, insbesondere Betriebs- und Geschäftsgeheimnisse, und für eine Zusammenfassung interner Besprechungen. Jedenfalls offene KI-Anwendungen sind für die Verarbeitung solcher Informationen regelmäßig nicht geeignet. Gleiches gilt für Personaldaten, also Daten, die zur Abwicklung des Beschäftigtenverhältnisses verarbeitet werden.

Neben inhaltlichen Fragen sind immer auch organisatorische Belange zu klären: Wer darf den Einsatz freigeben, welche Anwendungen werden eingesetzt, wann erfolgt eine Evaluation, wie wird der Einsatz dokumentiert und Transparenz hergestellt?

Der NDR hat sich mit diesen Fragen auseinandergesetzt, **KI-Leitlinien** erstellt und den Prozess zur Freigabe der Nutzung in einer Taskforce kanalisiert.

Bereits vor der Befassung mit KI gab es die Notwendigkeit, **Inhalte zu klassifizieren, um Risiken zu vermeiden**. Nicht alle Informationen können in allen verfügbaren Systemen verarbeitet werden. Der Prozess der Erprobung von KI hat dazu geführt, dass die Klassifikation und der Umgang mit Informationen noch stärker in den Fokus gerückt sind. Ein einheitliches Verständnis von Begriffen wie „vertraulich“ oder „sensibel“ ist umgangssprachlich kaum herzustellen. Zu unterschiedlich

sind die jeweils persönlichen Wertungen. Die Datenschutzbeauftragten und IT-Sicherheitsbeauftragten des öffentlich-rechtlichen Rundfunks haben daher eine Grundlage geschaffen, die diese Dinge übergreifend vereinheitlichen sollen:

Um Informationen angemessen zu schützen, ist es erforderlich, den jeweiligen **Grad der Vertraulichkeit zu klassifizieren** und die für die entsprechende Schutzklasse definierten, notwendigen technischen und organisatorischen Schutzmaßnahmen umzusetzen. Die Klassifizierung orientiert sich an den relevanten Bedrohungen und dem möglichen Schaden, den eine missbräuchliche Nutzung von Informationen - z. B. durch einen Informationsabfluss oder eine ungewollte Veröffentlichung - verursachen könnte. Daraus können Risiken resultieren, die rechtlicher, geschäftlicher, technischer oder strategischer Art sein können.

Die Informationsklassen

- öffentlich,
- Dienstgebrauch,
- vertraulich und
- streng vertraulich

wurden daher definiert, kategorisiert, durch Beispiele erläutert und einem Schutzbedarf zugeordnet. Für alle Verarbeitungsarten, also das

- Erheben/Erstellen/Ändern,
- Aufbewahren/Speichern,
- Übermitteln und
- Löschen/Vernichten

wurden Anforderungen nach einem **Ampel-System** definiert, um einen umfassenden Schutz zu gewährleisten. **Die Harmonisierung von „Vorstellungen“ zur Vertraulichkeit, Sensibilität und Sicherheit** muss nun weiter vorangebracht werden, um diesbezügliche Unsicherheiten zu nehmen und die vielen kleinen diesbezüglichen Anfragen durch ein einheitliches Grundverständnis zu klären.

Wenn eingangs formuliert wurde, dass ein „einheitliches Begriffsverständnis von bestimmten Informationen übergreifend hergestellt und Informationen klassifiziert werden [müssen], damit in den zahlreichen technischen Systemen die Persönlichkeitsrechte von betroffenen Personen gewahrt bleiben und Informationen richtig, sicher und rechtmäßig verarbeitet werden“, dann ist damit genau der soeben abgebildete Prozess gemeint. **Der NDR sollte rasch dafür sorgen, dass die Umsetzung umfassend vorgenommen und ein einheitliches Sprachverständnis etabliert wird**. Dies gilt nicht nur für den Einsatz von KI-Anwendungen, sondern für alle Verarbeitungssituationen. Die Ampel muss also eingeschaltet werden.

6. Weitere Beratungen und Prüfungen

Fast alles, was beschafft, erneuert und in Betrieb genommen wird, stellt eine Datenverarbeitung dar. Regelmäßig sind daher Anfragen eingetroffen, die aus allen Bereichen des NDR stammen. Um die Zielsetzung datenschutzrechtlicher Vorgaben zu erreichen, wurde auf die jeweils einschlägigen Anforderungen hingewiesen.

Hinsichtlich der Dokumentation dieser Verarbeitungen hat sich im Laufe des Jahres herausgestellt, dass insoweit weiterhin Schulungsbedarf besteht, als zu oft angenommen wurde, dass die Prozesse keine Verarbeitungen personenbezogener (Beschäftigten-) Daten darstellten. Das entsprechend zu führende **Verfahrensverzeichnis gemäß Art. 30 DSGVO** ist daher vom Verantwortlichen nachzuarbeiten und bestenfalls so zu gestalten, dass eine Inbetriebnahme von Anwendungen ohne einen entsprechenden Eintrag nicht möglich ist.

a) Organisations- und Strukturprojekte

Auszugsweise gab es beratende Tätigkeiten hinsichtlich der folgenden Vorhaben und Anwendungen des NDR:

- Erneuerung von Übertragungstechniken aus Landtagen
- Digitalisierung der Entgeltabrechnungen
- Crossmediale Übertragungswagen

- Studiotechniken und Redaktionssysteme
- Desksharing Buchungstool
- Digitale Arbeitszeiterfassungen
- Konferenzraumtechniken
- Managementsysteme für Kundenkontakte und Communities
- Sendeabwicklungen
- Authentifizierungsanforderungen
- Interne Suchmaschinen
- Forensische IT-Untersuchungen
- Technik- und Studioersatze
- Crossmediale Rechtemanagement-Systeme
- Mobile Produktionsnetzwerke
- Aufgaben- und Workflowmanager
- Verleihstationen für Audio-/Videoausrüstungen
- Videoüberwachungen
- Fernschnitt
- Hybrider Postversand
- Medienbildungsangebote für Schulklassen

Und auch im Jahr 2024 gab es **rund 100 Begutachtungen** von IT-Anwendungen und Prototypen aus datenschutzrechtlicher Perspektive.

b) Datensicherheit

Die Lage der IT- und damit auch Datensicherheit in Deutschland (und weltweit) ist besorgniserregend. Zu diesem Befund kommt das Bundesamt für Sicherheit in der Informationstechnik (BSI) leider schon seit Jahren: „Gezielte Cyberattacken gegen staatliche wie politische Institutionen und KI-geboostete Desinformationskampagnen werten wir als Angriffe auf unsere Demokratie, gegen die wir uns entschieden zur Wehr setzen. Angriffe mit Ransomware, sogenannte Verschlüsselungstrojaner, haben erneut zahlreiche Kommunen und damit unmittelbar Bürgerinnen und Bürger getroffen. Auch unzählige Unternehmen sind auf diesem Wege zu Opfern cyberkrimineller Täter geworden. Es ist unabdingbar, dass wir uns – Kommunen und Unternehmen sich selbst – besser schützen. Gleiches gilt für Angriffe mit dem Ziel der

Cyberspionage. Nicht zuletzt werden DDoS-Angriffe (Überlastangriffe) weiterhin insbesondere von Unterstützern des völkerrechtswidrigen russischen Angriffskrieges genutzt, um – im Wesentlichen – Propagandaeffekte zu erzielen“ (BSI, Die Lage der IT-Sicherheit in Deutschland 2024).

Dieser zusammengefasste Befund spricht zugleich Maßnahmen an: Sicherheit ist eine Gemeinschaftsaufgabe und damit zugleich eine solche, die auch selbst geleistet werden muss. Technische und organisatorische Maßnahmen sind zu ergreifen, um unbefugte Zugriffe Dritter abzuwehren. Diese ergreift auch der NDR unter Einbezug des Rundfunkdatenschutzbeauftragten, etwa durch Awareness-Kampagnen und Techniken der Angriffserkennung und -abwehr.

F. Anfragen nach dem Informationszugang

Im Jahr 2024 wurden rund 40 Anfragen auf Informationszugang an den NDR gerichtet. Damit hat sich die Zahl mehr als verdoppelt. Auch die Anrufung des Rundfunkdatenschutzbeauftragten als Beschwerdestelle hat sich entsprechend erhöht.

Beschwerden gab es unter anderem, weil manche anfragenden Personen auch auf Nachfrage des NDR anonym bleiben wollten. Diesbezüglich gilt:

Anspruch auf Informationen nach § 47 Abs. 1 NDR Staatsvertrag haben natürliche oder juristische Personen mit Sitz in Deutschland. Die Prüfung der Anspruchsberechtigung bezieht sich mithin neben dem Inhalt der beantragten Information auch auf die anfragende Person und deren Wohnsitz. Dies gilt insbesondere für den Fall einer teilweisen Ablehnung des Ansinnens, weil sich daran Rechtswegfolgen knüpfen. Die Erhebung entsprechender Daten (Namen, vollständige Anschrift) ist folglich nicht rechtsgrundlos, sondern resultiert aus einer rechtlichen Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c) DSGVO), weil Entscheidungen über derartige Auskünfte grundsätzlich durch Verwaltungsakt zu erfolgen haben (vgl. OVG NRW, Az. 5 A 166/10, Urt. vom 09.02.2012: „Damit steht dem Beklagten auch kraft Gesetzes die Befugnis zu, durch Verwaltungsakt über Informationszugangsbegehren zu entscheiden.“).

Für den NDR hat dies einen konkreten Niederschlag in § 47 Abs. 1 und 6 NDR Staatsvertrag gefunden. Denn Art. 47 Abs. 6 NDR Staatsvertrag lautet: „Der oder die Antragstellende ist im Falle einer vollständigen oder teilweisen Ablehnung eines Antrages über die Rechtsschutzmöglichkeiten gegen diese Entscheidung sowie darüber zu belehren, bei welcher Stelle und innerhalb welcher Frist um Rechtsschutz nachgesucht werden kann.“ Nach § 47 Abs. 7 NDR Staatvertrag ist der Verwaltungsrechtsweg eröffnet. Zwecks der gesetzlich geforderten Belehrung über den Rechtsschutz sind daher die Kenntnis und entsprechende Verarbeitung der Daten (Person und Anschrift) notwendig, weil dies für die Zuständigkeit der Gerichte maßgeblich ist (§ 52 VwGO).

G. Fazit und Ausblick

Die Welt ist komplex, es wimmelt nur so von Informationen, und die jeweiligen Beschreibungen von Sachverhalten und die Auffassungen dazu sind zahlreich. Eine Reduktion von Komplexität ist erforderlich, wozu extreme oder populistische Positionen sicherlich nicht taugen. Weglassungen oder Vereinfachungen reduzieren nicht die Komplexität, sondern Verzerren und Verfälschen. Es gilt vielmehr, intelligente Maßnahmen zu ergreifen, Menschen zu befähigen, Strukturen zu festigen und Prozesse sicher zu steuern, um die Komplexität einzufangen und die Informationen richtig zu verarbeiten. Zumindest derzeit ist Künstliche Intelligenz kein Ersatz für diese Maßnahmen, sondern eine Steuerungsaufgabe. Wenn „KI wahrscheinlich das Beste oder das Schlimmste [ist], was der Menschheit passieren kann“, so Stephen Hawking, sollte das Beste daraus gemacht werden. Man könnte ergänzen: „Prüft alles und behaltet das Gute!“ (1. Thessalonicher 5,21). Datenschutz kann diesen Prozess mitsteuern und zumindest das Schlimmste verhindern. Wie das u. a. gelingen kann, wurde in diesem Bericht in Ansätzen dargelegt.

Begonnen wurde dieser Bericht mit einem Zitat aus dem Bericht des Hessischen Datenschutzbeauftragten aus dem Jahr 1972, und so schließen auch diese Ausführungen mit einem Zitat von ebenda, das an Aktualität kaum zu übertreffen ist – es passt maßgeschneidert insbesondere auf Künstliche Intelligenz:

„Es gibt keine — oder bestenfalls nur eine für jeweils kurze Zeit geltende — perfekte Lösung für den Datenschutz. Denn die Entwicklung steht nicht still. Neue Techniken werden vielleicht schon morgen neue Wege zum Fortschritt und zum Wohl des Menschen erschließen; aber sie werden auch neue, unbekannte Gefahren für den einzelnen und für die freiheitliche Struktur von Staat und Gesellschaft in sich bergen. Diesen Gefahren muß rechtzeitig und wirksam entgegengetreten werden. Stete Wachsamkeit ist notwendig. Auch die Gesellschaft wird ihre Strukturen wandeln. Neue Bedürfnisse und Auffassungen werden auch Fragen des Datenschutzes berühren. Datenschutz ist deshalb keine einmalige, sondern eine permanente Aufgabe, die jeden Tag aufs neue gestellt wird und die es gilt, jeden Tag neu zu überdenken.“