NORDDEUTSCHER RUNDFUNK

Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten des NDR

für das Berichtsjahr 2025

Dr. Heiko Neuhoff

Hamburg im Januar 2026

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 2025.

Danksagung

Meiner Mitarbeiterin sei für die Unterstützung des Rundfunkdatenschutzbeauftragten des NDR in allen Angelegenheiten herzlich gedankt.

Inhalt

A. Einleitung

Vor 40 Jahren, also im Jahr 1986 erschien das Buch „Risikogesellschaft - Auf dem Weg in eine andere Moderne“ des Soziologen Ulrich Beck. Dieser Klassiker der Soziologie beschrieb die postindustrielle Gesellschaft und ihren Übergang in eine risikobehaftete Moderne, die von Ungewissheiten und Unsicherheiten geprägt ist. Nicht nur aufgrund der Nuklearkatastrophe von Tschernobyl, sondern auch wegen der fortschreitenden Verschmutzung der Umwelt werden beispielsweise Risiken wie naturwissenschaftliche Schadstoffverteilungen und der gesellschaftliche Umgang damit beschrieben. Auch soziale Gefährdungslagen, etwa Arbeitslosigkeit und der Bedeutungsverlust tradierter sozialer Bindungen, sind Gegenstand des Werkes. Letztlich, so Beck, seien Risiken und deren Bedeutung und Behandlung auch stets das Ergebnis von gesellschaftlichen Konstruktionsprozessen in der Thematisierung durch die Massenmedien.

Schon vor 40 Jahren konnte festgestellt werden: Risiken „besitzen eine immanente Tendenz zur Globalisierung. Mit der Industrieproduktion geht ein Universalismus der Gefährdungen einher, unabhängig von den Orten ihrer Herstellung. Sie tauchen unter Grenzen durch.“

Konsequenterweise erschien im Jahr 2008 das Werk „Weltrisikogesellschaft – Auf der Suche nach der verlorenen Sicherheit“, ebenfalls von Ulrich Beck. Die identifizierten Risiken hatten sich nicht nur weiter globalisiert, sondern fortentwickelt oder verlagert. Dabei wird auch die **technische Entwicklung** verstärkt in den Blick genommen: „Der Übergang von der Industrie- zur Risikoepoche der Moderne vollzieht sich ungewollt, ungesehen, zwanghaft im Zuge der Modernisierungsdynamik nach dem Muster der latenten Nebenfolgen.“ Die Risikogesellschaft ist also keine gewählte Option, sondern die Gefährdungen erzeugen sich von selbst. Die technische Entwicklung, heute maßgeblich die informationstechnische, ist untrennbar mit gesellschaftlichen und globalen Folgen verbunden, wobei der Gesetzgeber versucht, Risiken zu regulieren:

„Die Zentralstellung des Staates in der materiellen Förderung und politischen Regulierung von technischem Fortschritt hat politischen Institutionen eine wichtige Rolle bei der Haftung für Fortschrittsfolgen gegenüber der Gesellschaft zuwachsen lassen. Der technische Fortschritt und seine Folgen haben so Kollektivgütercharakter angenommen.“

Schon die Datenschutzgrundverordnung (DSGVO) folgt einem **risikobasierten Ansatz**, auch wenn sich in dem Regelwerk keine Definition des Risikos finden lässt. In verschiedenen Vorschriften wird das Risiko mitgedacht und die Verantwortlichen verpflichtet, risikominimierende Maßnahmen zu ergreifen, etwa wenn eine Datenverarbeitung „insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat (Art. 35 DSGVO).

Nach entsprechenden Grundannahmen hat der europäische Gesetzgeber auch Risikoeinschätzungen vorgenommen und Haftungsfragen beantwortet, als er die europäische Verordnung über künstliche Intelligenz (KI-Verordnung) erließ. Denn Techniken sind keine risikoarmen Anwendungen gesicherten Wissens mehr, sondern produzieren neben Chancen auch Risiken. Die EU-Kommission sieht daher die KI-Verordnung als Risikobewältigungsrahmen:

„Sie [die KI-Verordnung] ist insbesondere auf die potenziellen Risiken von KI für die Gesundheit, die Sicherheit und die Grundrechte der Bürgerinnen und Bürger ausgerichtet. Die Verordnung legt klare Anforderungen fest, die KI-Entwickler und -Betreiber je nach der spezifischen Verwendung der KI zu erfüllen haben, und verringert gleichzeitig den administrativen und den finanziellen Aufwand für Unternehmen.

Mit der KI-Verordnung wird ein einheitlicher Rahmen für alle EU-Länder eingeführt, der auf einer zukunftsgewandten Begriffsbestimmung für KI und einem risikobasierten Ansatz beruht.“

Der Begriff des Risikos und der Risikoregulierung haben also eine jahrzehntelange Geschichte und die „Erfolgsgeschichte“ der Risiken dürfte anhalten. Globale Risiken entfalten sich durch Aggressionen, Unsicherheiten, knappe Ressourcen, aber auch durch Abhängigkeiten. Die Rundfunkdatenschutzkonferenz, über deren Tätigkeit noch berichtet wird, hatte in einer Veröffentlichung vom August 2025 den internationalen bzw. transatlantischen Datenverkehr betreffend dies formuliert:

„**Empfehlungen zur Sicherung der digitalen Souveränität:**
Um die digitale Souveränität und die Datensicherheit zu sichern und um das europäische Datenschutzniveau zu erhalten, empfiehlt die RDSK den Anstalten folgende Maßnahmen:

- Aufbau einer eigenen, unabhängigen digitalen Infrastruktur,

- Einsatz von Open-Source-Software – wo immer dies möglich ist,
- Nutzung und Förderung europäischer Cloud-Lösungen,
- Kompetenzaufbau/Investitionen in Aus- und Weiterbildung,
- Zusammenarbeit mit anderen öffentlichen Einrichtungen und politisches Engagement für die europäische digitale Souveränität im Hinblick auf die Sicherung der Rundfunkfreiheit in Deutschland und Europa,
- Ausprägung einer Hybridstrategie (europäische Clouds, On-Premise-Lösungen),
- Erarbeitung von Strategien zur Rückholbarkeit von Daten,
- Bereitstellung von Notfall- und Krisenmaßnahmen.

Wirksame Maßnahmen zum Aufbau und Schutz der digitalen Souveränität und damit nicht zuletzt zur Gewährleistung der Unabhängigkeit der Rundfunkanstalten müssen angesichts der weltpolitischen Lage als unabdingbar angesehen werden“ (https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/empfehlung-der-rdsk-zum-umgang-mit-dem-angemessenheitsbeschluss-fuer-den-datenschutzrahmen-zwischen-der-europaeischen-union-und-den-usa).

Grund für diese Empfehlung war und ist die sich ausweitende Abhängigkeit des öffentlich-rechtlichen Rundfunks von nicht-europäischen Dienstleistern und die damit einhergehenden Risiken für den Schutz (sensibler) personenbezogener und anderer Daten. So hat beispielsweise eine Studie der Universität zu Köln, die im Auftrag des Bundesinnenministeriums erstellt wurde, mit dem Titel „Rechtsgutachten zur US-Rechtslage zum weltweiten Datenzugriff durch US-Behörden bei Nutzung von Cloud-Diensten“ ermittelt, dass US-Behörden einen weitreichenden Zugriff auf Informationen auch dann haben können, wenn der Speicherort in europäischen Rechenzentren ist (https://fragdenstaat.de/dokumente/273689-rechtsgutachten-zur-us-rechtslage_geschwaerzt/).

Immerhin ist dieses Thema ein solches, das verstärkt in den öffentlichen Fokus gerät. Der „Gipfel zur europäischen digitalen Souveränität“ am 18. November 2025 in Berlin soll einen „Startschuss für ein eigenständigeres Europa“ geben mit dem Ziel, mehr digitale Unabhängigkeit zu erlangen, Investitionen in Technologien zu fördern und europäische Lösungen zu finden, um im digitalen Raum weniger dem Risiko der Abhängigkeit von Dritten ausgesetzt zu sein (https://www.bundesregierung.de/breg-de/aktuelles/digitale-souveraenitaet-2394250). Ob dies gelingen wird und ob die durch den **digitalen Omnibus** (dazu sogleich) in Aussicht genommene Deregulierung neue Risiken entstehen, bleibt abzuwarten.

Nicht nur die Abhängigkeit kann ein Risiko darstellen, sondern auch die „**KI-Ära**“. Eine Jury der Gesellschaft für deutsche Sprache (GfdS) hat diesen Begriff zum Wort des Jahres 2025 gekürt (https://gfds.de/worter-des-jahres-2025/). Begründung: „Die Künstliche Intelligenz (KI) ist aus dem Elfenbeinturm der wissenschaftlichen Forschung herausgetreten und hat die Mitte der Gesellschaft erreicht. Ob bei Recherchen im Internet, bei der Animation von Fotos oder bei der Erstellung von Texten: Immer mehr Menschen nutzen heutzutage Werkzeuge Künstlicher Intelligenz. Auch schon in den zurückliegenden Jahren war das Thema bei der Wahl der Wörter des Jahres erkennbar geworden. […] Aus Sicht der GfdS ist der Beginn einer *Ära* nicht zu verkennen – mit vielen Chancen, aber ebenso mit Risiken des Missbrauchs und eines Verlustes an eigenständigem, kritischem Denken, Sprechen und Schreiben.“

Auch in den USA wurde ein Wort des Jahres gekürt. Dort ist der Begriff „**Slop**“ das Wort des Jahres. Übersetzt bedeutete dies früher „weicher Schlamm“. Gemeint ist damit aber etwas von geringem Wert („Trash“). Der Begriff wird heute verwendet für digitalen Content, der regelmäßig unter Einsatz von KI erstellt wird: Merkwürdige Videos und Bilder, überzogene Propaganda, sonstige Inhalte von minderwertiger Qualität und gefälschte Nachrichten. Hier ein Beispiel eines harmlosen Slops:

Die zuletzt genannten gefälschten Nachrichten – Fake News – stellen, im Gegensatz zu comichaften Tieren in Weltraumanzügen, wiederum auch ein Risiko dar. Auf weitere Risiken, die aus dem Einsatz von KI resultieren, wird im Laufe des Berichts noch eingegangen.

Festzuhalten bleibt an dieser Stelle: Generell auszuschließen sind Risiken jeweils nicht, sie sind fortschrittsimmanent. Risiken sind versicherbar, manchmal vorhersehbar und damit zumindest eingrenzbar. Einen Beitrag zur Eingrenzung von Risiken kann eine **effiziente Organisation des Datenschutzes** leisten und darüber hinaus sogar zur Entfaltung von Potenzialen beitragen. Dies hat eine Studie der französischen Datenschutzaufsichtsbehörde CNIL gezeigt. Die Untersuchung befasst sich zwar im Kern mit den wirtschaftlichen Vorteilen für Unternehmen mit einer guten Datenschutzorganisation. Sie ermittelte aber auch weitere Vorzüge, wie etwa Vermeidung von sanktionsfähigen Verletzungen, Kostenersparnisse und vertrauensbildende Maßnahmen (https://www.cnil.fr/fr/quels-benefices-economiques-du-dpo-en-entreprise).

B. Rechtsgrundlagen und Zuständigkeiten des Rundfunkdatenschutzbeauftragten des NDR

Änderungen hinsichtlich des rechtlichen Rahmens und der Aufgaben gab es nicht. Daher folgt ein Zitat aus dem Tätigkeitsbericht für das Jahr 2024:

„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

Auch hinsichtlich der personellen Besetzung herrschte Kontinuität: Der Rundfunkdatenschutzbeauftragte übt seine Tätigkeit seit dem 25. Mai 2022 in der zweiten Amtszeit aus, anteilig unterstützt durch eine Assistenz. Zudem war der Rundfunkdatenschutzbeauftragte des NDR stellvertretender Vorsitzender 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

Es folgt ein ausschnittsweiser Überblick über wesentliche Entwicklungen auf dem Gebiet des Datenschutzes sowie ein Blick in die Zukunft.

I. EU-Kommission

Im November 2025 kündigte die Kommission an, dass mehrere europäische Rechtsvorschriften überarbeitet und zusammengefasst werden sollen. Der schon erwähnte digitale Omnibus soll verschiedene Regelwerke, unter anderem die DSGVO und die KI-Verordnung, erneuern und zusammenfassen. Ein Vorschlag dazu liegt bereits vor und wird wie folgt erläutert und begründet:

„Der Vorschlag für einen digitalen Omnibus enthält eine Reihe technischer Änderungen an einem großen Korpus digitaler Rechtsvorschriften, die ausgewählt wurden, um Unternehmen, öffentlichen Verwaltungen und Bürgern gleichermaßen Soforthilfe zu bieten und die Wettbewerbsfähigkeit zu fördern.

Dies ist ein erster Schritt zur Optimierung der Anwendung des digitalen Regelwerks. Das unmittelbare Ziel besteht darin, sicherzustellen, dass die Einhaltung der Vorschriften zu geringeren Kosten erfolgt, die gleichen Ziele erreicht und verantwortungsvollen Unternehmen einen Wettbewerbsvorteil verschafft“
(https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-regulation-proposal).

Es bleibt abzuwarten, welche Inhalte des Vorschlags in Gesetzeskraft erwachsen und inwieweit auch der öffentlich-rechtliche Rundfunk betroffen sein wird. Nach aktuellem Stand des Vorschlags soll jedenfalls auch die Datenschutzgrundverordnung von der Novellierung tangiert sein, weil im Kern eine erleichterte Datennutzung angestrebt wird.

Derzeit besteht jedenfalls die nachvollziehbare Befürchtung, dass das aktuelle Schutzniveau von Personen, deren Daten verarbeitet werden, sinkt. Denn Vorschriften zur Kontrolle und damit Souveränität über Datenverarbeitungen könnten gestrichen oder im Geltungsumfang eingeschränkt werden. Angedacht ist auch, die als besonders schützenswert geltenden Daten des Art. 9 DSGVO (etwa Gesundheitsdaten, Informationen, die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die sexuelle Orientierung betreffend) weniger streng zu regulieren

(https://netzpolitik.org/2025/digitaler-omnibus-eu-kommission-will-datenschutzgrundverordnung-und-ki-regulierung-schleifen/).

Außerdem sollen Daten in vereinfachter Weise zum Trainieren von KI-Modellen genutzt werden. Noch gilt aber die KI-Verordnung und seit dem 2. Februar 2025 sind bestimmte hochriskante KI-Praktiken verboten (Art. 5 KI-VO), und zwar solche mit erheblichen Gefahren für Grundrechte, Sicherheit und gesellschaftliches Zusammenleben. Dazu zählen etwa manipulative KI-Anwendungen, Social Scoring-Systeme und biometrische Kategorisierungssysteme. Zur Konkretisierung hat die EU-Kommission Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz veröffentlicht, die für Unternehmen und Behörden Rechtssicherheit schaffen sollen (zu finden unter https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act).

II. Der Europäische Datenschutzausschuss (EDSA)

Der EDSA, also das unabhängige europäische Gremium, dessen Mitglieder die nationalen Datenschutzbehörden des Europäischen Wirtschaftsraums und der Europäische Datenschutzbeauftragte sind, hat sich mit der Entwicklung und dem Einsatz von KI-Modellen befasst. Jedenfalls nicht im Einklang mit der zuvor genannten Absicht der EU-Kommission im digitalen Omnibus, geht der EDSA davon aus, dass Personen grundsätzlich nicht damit rechnen müssen, dass ihre personenbezogenen Daten – auch wenn sie im Internet auffindbar sind - uneingeschränkt für das Training von KI-Modellen verwendet werden
(https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf).

Der EDSA geht davon aus, dass KI-Modelle in der Regel personenbezogene Daten enthalten, auch wenn vollständig anonyme KI-Modelle denkbar seien. Mit personenbezogenen Daten trainierte Modelle unterfielen aber dem Datenschutzrecht. Um Rechtssicherheit bei der Nutzung von KI-Modellen zu erlangen, soll ein Test helfen. Im öffentlich-rechtlichen Rundfunk ist der „**Drei-Stufen-Test**“ nicht unbekannt, und auch für den Einsatz von KI wird ein dreistufiger Test empfohlen, in dem die Legitimität des Zwecks des Einsatzes geprüft, die Notwendigkeit der Datenverarbeitung festgestellt und schließlich eine Abwägung der Interessen aller Beteiligten durchgeführt wird

(https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_de).

III. Nationale Gesetzgebung

Am 1. Dezember 2025 trat der **Reformstaatsvertrag** in Kraft. Dieser 7. Medienänderungsstaatsvertrag bringt eine Reihe von Änderungen auch den Datenschutz betreffend mit sich, auf die im Laufe des Berichts noch eingegangen wird. An dieser Stelle sei lediglich erwähnt, dass es zu einer vermehrten Verarbeitung personenbezogener Daten von Nutzenden der digitalen Angebote des öffentlich-rechtlichen Rundfunks kommen dürfte. Denn der Gesetzgeber will – etwa durch § 30 f ReformStV („Gemeinsames technisches Plattformsystem") **Personalisierungsmöglichkeiten und Empfehlungssysteme** vorantreiben und eine **Nutzungs- und Leistungsanalyse** etablieren. Dabei soll eine „besondere Verantwortung bei der Datenverarbeitung" vorherrschen (§ 31 i ReformStV), bei der „die in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF und das Deutschlandradio zu einem sorgsamen Umgang mit personenbezogenen Daten von Nutzern verpflichtet [werden]. Sie dürfen diese verarbeiten, soweit dies zum Zwecke der Auftragserfüllung erforderlich ist. Ein Austausch personenbezogener Daten von Nutzern zwischen den in der ARD zusammengeschlossenen Landesrundfunkanstalten, dem ZDF und dem Deutschlandradio ist, sofern diese auf der Basis des gemeinsamen technischen Plattformsystems zur Verwirklichung des gemeinwohlorientierten öffentlichen Raum nach § 30 Abs. 1 Satz 2 verarbeitet werden, Teil des Auftrags."

Mit § 26 a ReformStV wird auch eine Leistungsanalyse eingeführt, für die der Gesetzgeber eine „datengestützte Überprüfung der eigenen Leistung mit Blick auf die Auftragserfüllung" errichtet. Welche Daten in welcher Weise erhoben werden, ist noch zu konkretisieren. In der Begründung des ReformStV heißt es dazu: „Hierdurch wird der öffentlich-rechtliche Rundfunk gerade auch bei der Weiterentwicklung seiner Angebote noch stärker auf seinen Beitrag zur demokratischen Selbstverständigung verpflichtet und dazu, eine gemeinsame, faktengestützte Diskussionsebene für die gesamte Gesellschaft (z.B. Stadt und Land, in den Regionen, Alt und Jung, verschiedene Bildungsniveaus, Menschen mit und ohne Migrationshintergrund) zu schaffen."

IV. Rechtsprechung

Die Rechtsprechung zu datenschutzrechtlichen Themen wird immer detaillierter und umfangreicher. Der folgende Überblick ist daher bereits stark eingeengt auf einige wesentliche Entscheidungen.

1. (Negative) Gefühle

Gelegentlich wird „der Datenschutz“ als sperrig und vielleicht auch langweilig abgetan. Das neu eingerichtete **Datenbarometer** der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat noch weitere „Haltungen“ zum Datenschutz in einer repräsentativen Umfrage ermittelt. Einige der Befragten konnten positive Verbindungen herstellen („Sicherheit, Schutz Privatsphäre“), andere waren unentschieden („Fluch und Segen zugleich“) und eine weitere Gruppe zeigte sich kritisch oder leider auch desillusioniert (https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/15_Datenbarometer.html).

Datenschutz weckt also Emotionen. Dies auch unter anderem dann, wenn es um die Einforderung eines immateriellen Schadensersatzes geht. Hier stehen Gefühle im Mittelpunkt, auch wenn es um solche wie eine Befürchtung oder eine Besorgnis geht.

Bereits im vorangegangenen Tätigkeitsbericht ging es an dieser Stelle um die Frage, unter welchen Voraussetzungen ein immaterieller Schaden vorliegt, der auch zu einem Schadensersatz führt. Die Gerichte hatten sich immer wieder mit der Frage zu befassen, wann der Anspruch auf immateriellen Schadensersatz besteht. Und tatsächlich können nach der Rechtsprechung des Gerichtshofs der Europäischen Union **negative Gefühle** wie etwa Befürchtungen in bestimmten Konstellationen einen Anspruch auf Ersatz des immateriellen Schadens begründen. Zwar reicht das bloße Berufen auf eine solche Gefühlslage nicht aus, um einen Schadensersatz zu begründen. Vielmehr ist zu ermitteln, ob das schlechte Gefühl tatsächlich unter Berücksichtigung der konkreten Umstände „als begründet angesehen werden kann“ (EuGH, Urteil vom 14.12.2023 - C-340/21 - [Natsionalna agentsia za prihodite] Rn. 85). Gefühle müssen also objektiviert werden, wobei es allerdings keine Bagatellgrenze gibt. Das Bundesarbeitsgericht hat beispielsweise dazu diese Lösung gefunden:

„Besteht der Schaden in negativen Gefühlen, die für sich genommen nicht beweisbar sind, hat das nationale Gericht die Gesamtsituation und letztlich auch die Glaubwürdigkeit der jeweiligen Klagepartei auf der Grundlage eines substantiierten Sachvortrags zu beurteilen. Steht ein Verstoß gegen die Datenschutzgrundverordnung […] nach richterlicher Beweiswürdigung […] zum Nachteil der Klagepartei als geschützter Person fest, mindert sich das Beweismaß bzgl. der Entstehung und der Höhe des Schadens“ (Bundesarbeitsgericht, Urteil vom 20.06.2024, Az. 8 AZR 91/22). Auf dieser Linie liegen auch die zahlreichen weiteren Entscheidungen der Gerichte, die im Berichtsjahr dazu ergangen sind.

2. KI-Training

Das OLG Köln hat entschieden, dass Meta personenbezogene Daten von volljährigen Personen für das Training eigener KI-Anwendungen grundsätzlich verwenden darf. Dies aber nur dann, wenn es sich um öffentliche Posts handelt und ein ausreichender Schutz der Betroffenen gewährleistet ist (OLG Köln, Urteil vom 23.05.2025, Az. 15 UKl 2/25).

Das Vorhaben war auf Kritik gestoßen, weil nicht sichergestellt sei, dass besonders sensible Daten (etwa bezüglich Herkunft, Religion, Gesundheit oder sexueller Orientierung) vom Training ausgeschlossen werden könnten. Das Gericht fand dies jedoch unbedenklich, weil die betroffenen Personen diese Informationen offensichtlich selbst öffentlich gemacht hätten.

3. Facebook-Fanpage

Zitat aus dem Tätigkeitsbericht für das Jahr 2023:

„Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hatte mit einem Bescheid vom 17.02.2023 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 Urteil des VG Köln vom 17.06.2025 (Az. 13 K 1419/23) schließt die Sache nicht endgültig ab, weil das Gericht die Berufung zugelassen hat und bereits die Fortsetzung des Verfahrens durch die BfDI angekündigt wurde. Der aktuelle Stand ist, dass das BPA seine Fanpage weiterbetreiben darf. Die Untersagungsverfügung aus dem Jahr 2023 wurde aufgehoben. Das Gericht begründet seine Entscheidung wie folgt:

„Nicht das Bundespresseamt, sondern allein „Meta“ ist zur Einholung einer Einwilligung der Endnutzenden für die Platzierung von „Cookies“ verpflichtet. Es besteht kein ausreichender Ursachen- und Wirkungszusammenhang zwischen dem Betrieb der „Fanpage“ durch das Bundespresseamt und dem mit der Speicherung und dem Auslesen der „Cookies“ verbundenen Fernzugriff auf die Endgeräte der Nutzer. Die „Cookies“ können zwar bei Gelegenheit des Besuches einer „Fanpage“, ebenso jedoch bei dem Besuch einer jeden anderen „Facebook-Seite“ platziert werden“ (https://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/08_22072025/index.php).

Wie bereits erwähnt, ist das letzte Wort in dieser Sache noch nicht gesprochen. Berufung wurde eingelegt, verbunden mit dieser Ankündigung der BfDI:

„Ich möchte die Rechtsunsicherheit bei der Nutzung sozialer Medien durch öffentliche Stellen des Bundes beenden. Deswegen veröffentlichen wir heute eine Handreichung, die die notwendigen Schritte darstellt, um Behörden eine rechtssichere Nutzung sozialer Netzwerke zu ermöglichen. […] Selbstverständlich sehen wir, wie wichtig es für den Staat geworden ist, auf sozialen Netzwerken zu kommunizieren. Welche Bedingungen dafür gelten, ist aber bislang völlig unklar und kann nur entweder durch den Gesetzgeber oder durch ein letztinstanzliches Urteil festgelegt werden.“

Auch wenn aufgrund des Medienprivilegs die Rechtslage bezüglich des öffentlich-rechtlichen Rundfunks etwas anders ist, sollte die weitere diesbezügliche Rechtsprechung im Blick behalten werden.

4. Transatlantischer Datenverkehr

Ein weiteres Zitat aus dem Tätigkeitsbericht für das Jahr 2023:

„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."

Das Urteil des Gerichts der Europäischen Union (EuG) vom 3. September 2025 (Rs. T-553/23) hat zwar wenig Aufmerksamkeit erhalten, ist jedoch von Bedeutung, weil es das genannte Abkommen und damit den entsprechenden Datenverkehr in die USA zum Gegenstand hatte. Das Gericht kam zu dem Schluss, dass die Vereinigten Staaten ein angemessenes Datenschutzniveau gewährleisteten (jedenfalls zum Zeitpunkt des Abschlusses des Abkommens). Die entsprechende Executive Order 14086 des damaligen Präsidenten Joe Biden und damit die Einrichtung eines unabhängigen Gremium in den USA bot betroffenen Personen in der EU wirksamen Rechtsschutz im Falle eines Transfers von personenbezogenen Daten in die USA.

Weil eine Vielzahl digitaler Anwendungen mit einem solchen Datentransfer verbunden ist, sollte – trotz aller Bemühungen um eine digitale Souveränität – dieses Thema wachsam verfolgt werden.

5. EU-Kommission gegen EDSB

Ein letztes Zitat aus einem früheren Tätigkeitsbericht, diesmal aus dem für das Jahr 2024:

„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."

Diese Auseinandersetzung wurde beendet. Die EU-Kommission hatte diverse Maßnahmen ergriffen und dem EDSB nachgewiesen, sodass dieser die Umsetzung der Maßnahmen bestätigen konnte (https://www.edps.europa.eu/system/files/2025-07/25-07-11_letter-to-commission_2021-0518_en.pdf). Die Kommission hatte dafür diverse technische und organisatorische Maßnahmen ergriffen und vertragliche Anpassungen vorgenommen.

Auch die hiesigen Aufsichtsbehörden kamen im Laufe des Jahres zu dem Ergebnis, dass ein datenschutzkonformer Einsatz der Microsoft-Dienste möglich ist. So etwa der Hessische Beauftragte für Datenschutz und Informationsfreiheit:

„In den Verhandlungen konnte der HBDI feststellen, dass sich nach drei Jahren entscheidende Bedingungen geändert haben. Zum einen haben sich rechtliche Vorgaben verändert wie z.B. die Zulässigkeit der Übertragung personenbezogener Daten in die USA auf der Grundlage des EU-US Data Privacy Frameworks. Zum anderen hat MS seine Datenverarbeitung an europäische Anforderungen angepasst, wie z.B. durch die EU-Datengrenze, durch die MS fast alle personenbezogenen Daten im Europäischen Wirtschaftsraum verarbeitet. Drittens hat MS Veränderungen in seinem Datenschutzkonzept gegenüber dem HBDI ausführlich erläutert. Viertens konnte der HBDI erreichen, dass MS das DPA (für öffentliche Stellen) fortentwickelt hat. Schließlich stellt MS zusätzliche Informationen bereit wie z.B. das M365-Kit, das den Verantwortlichen bei seiner datenschutzrechtlichen Dokumentation unterstützt. Das positive Ergebnis beruht auch auf der Erwartung, dass MS und die Verantwortlichen zusammenwirken, damit Verantwortliche M365 datenschutzrechtskonform nutzen können“ (https://datenschutz.hessen.de/presse/hbdi-microsoft-365-kann-datenschutzkonform-genutzt-werden).

Da auch im öffentlich-rechtlichen Rundfunk diverse Microsoft-Produkte zur Anwendung kommen, sind diese und zukünftige Entwicklungen bedeutsam.

E. Tätigkeiten des Rundfunkdatenschutzbeauftragten des NDR im Jahr 2025

Es folgt zunächst eine Übersicht über die vernetzten Tätigkeiten innerhalb des öffentlich-rechtlichen Rundfunks und mit den staatlichen Aufsichtsbehörden. Anschließend werden die Tätigkeiten den NDR betreffend dargestellt.

I. Zusammenarbeit und Vernetzung

Die Vernetzungsstrukturen bestehen aus

- der **Rundfunkdatenschutzkonferenz** (RDSK (die als datenschutzrechtliche Aufsichtsbehörden tätigen Personen im öffentlich-rechtlichen Rundfunk, https://www.rundfunkdatenschutzkonferenz.de/)),
- dem **Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradios** (AKDSB (der Zusammenschluss aller Datenschutzbeauftragten von ARD, ZDF, Deutschlandradio, dem ORF, ARTE und der Schweizerischen Radio- und Fernsehgesellschaft)) und
- der **Datenschutzkonferenz** (DSK (das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, https://www.datenschutzkonferenz-online.de/)).

Außerdem gibt es ein Informationsangebot aller Datenschutzinstanzen, das Virtuelle Datenschutzbüro, das unter https://www.datenschutz.de/ Informationen zum Datenschutz bereitstellt.

1. Die Rundfunkdatenschutzkonferenz (RDSK)

Dieser Zusammenschluss der Aufsichtsbehörden über den öffentlich-rechtlichen Rundfunk und seine Gemeinschaftsangebote und Gemeinschaftseinrichtungen veröffentlicht seine Orientierungshilfen und Stellungnahmen unter https://www.rundfunkdatenschutzkonferenz.de/. Die Mitglieder erarbeiten arbeitsteilig die Veröffentlichungen und tauschen sich dazu regelmäßig aus. Grundlage der Zusammenarbeit sind die „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten“ und

die „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten“.

a) Tätigkeitsschwerpunkte der RDSK

Wie eingangs erwähnt, hat sich die RDSK veranlasst gesehen, ihre **Empfehlung zum Umgang mit dem Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union und den USA** zu überarbeiten. Die Aktualisierung war erforderlich, um trotz noch bestehender Abkommen auf mehr Sicherheit im transatlantischen Datenverkehr zu drängen. Denn obwohl einige amerikanische Unternehmen Bemühungen unternommen haben, ihre Datenverarbeitung von europäischen Kunden innerhalb des Geltungsbereiches der DSGVO vorzunehmen, gewährt der US-amerikanische Cloud Act (Clarifying Lawful Overseas Use of Data Act) aus dem Jahr 2018 den US-Behörden weitreichende Befugnisse, von amerikanischen Unternehmen Daten anzufordern, und zwar unabhängig davon, wo diese gespeichert sind. Daraus folgt, dass Daten, die in europäischen Rechenzentren gespeichert sind, auch von US-Behörden angefordert werden. Davon wären die Informationen von Rundfunkanstalten nicht ausgeschlossen. Die Empfehlung thematisiert dies und gibt Hinweise zum Schutz von Informationen. Diese münden in die oben erwähnten Ausführungen zur Sicherung der digitalen Souveränität.

Die zuletzt im September 2024 überarbeitete **Orientierungshilfe zum datenschutzkonformen Einsatz von KI im öffentlich-rechtlichen Rundfunk** hat einer Revision standgehalten. Die dortigen Ausführungen sind noch immer aktuell: https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen/orientierungshilfen/orientierungshilfe-zum-datenschutzkonformen-einsatz-von-ki-im-oeffentlich-rechtlichen-rundfunk.

Weitere Empfehlungen und Orientierungshilfen sind aufrufbar unter https://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen.

Die RDSK hat sich außerdem u. a. beschäftigt mit Dokumentationspflichten der Verantwortlichen für Auftragsverarbeiter, Anforderungen an den Redaktionsdatenschutz, dem Streaming und Aufzeichnung betrieblicher Versammlungen sowie den Auswirkungen des Reformstaatsvertrags.

b) Vernetzung der RDSK mit anderen Medienaufsichten

Der im Jahr 2024 aufgenommene Austausch der RDSK mit Aufsichtsbehörden über private Medien wurde fortgesetzt. Die Mitglieder der RDSK haben mit dem Medienbeauftragten für den Datenschutz Bayerische Landeszentrale für neue Medien (BLM) und der Beauftragten für Datenschutz der Landesanstalt für Medien NRW aktuelle Themen erörtert. So ging es um mehr Sichtbarkeit und eine bessere Vernetzung, aber auch wiederum um Fragen der digitalen Souveränität sowie um die Rolle der Datenschutzaufsichtsbehörden bei der Marktüberwachung nach der KI-Verordnung.

c) Austausch mit der Datenschutzkonferenz

Die **Datenschutzkonferenz** (DSK) lädt zweimal im Jahr zu einem Austausch ein. Mitglieder der RDSK und der datenschutzrechtlichen Aufsichtsbehörden der Kirchen und des privaten Rundfunks kommen (virtuell) zusammen, um über aktuelle Entwicklungen zu sprechen. Einsehbar sind die Protokolle der Sitzungen unter https://www.datenschutzkonferenz-online.de/protokolle.html.

Darüber hinaus genießen die Mitglieder einen Gaststatus in den Arbeitskreisen der DSK. Regelmäßig nehmen Mitglieder der RDSK teil an den Arbeitskreisen Medien, Grundsatzfragen und Technik. Hinzugekommen ist nun der Arbeitskreis KI.

Die Mitglieder der RDSK und der Kirchen betonen in diesem Zusammenhang regelmäßig, dass der Gaststatus zwecks Informationstransfers zwar begrüßenswert ist, jedoch eine Zusammenarbeit auf „Augenhöhe“ noch nicht erreicht sei, weil es an einer engeren Anbindung fehle.

d) Zukunft der RDSK

An dieser Stelle wurde im Bericht für das Jahr 2024 eingehend auf die Zukunft der RDSK ausgeführt. Ob und in welcher Zusammensetzung die RDSK fortgeführt wird, kann an dieser Stelle nicht gesagt werden. Da aufgrund § 31 j ReformStV die Datenschutzaufsicht über den öffentlich-rechtlichen Rundfunk mit

Ausnahme der Deutschen Welle zentralisiert wird, bestünde die RDSK nur noch aus zwei Mitgliedern.

Jedenfalls kann im Rückblick auf die kurz nach Inkrafttreten der DSGVO gegründete RDSK festgehalten werden, dass diese eine Reihe von Themen mit geringem Personalaufwand und hoher Effizienz begleitet hat.

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

Der AKDSB hat maßgeblich die Aufgabe der Beratung der Verantwortlichen in gemeinsam wahrgenommenen Tätigkeiten. Im Wesentlichen ging es um

- Anpassungen der Meldedatenübermittlungsverordnungen der Länder,
- Auswirkungen des Reformstaatsvertrags,
- Schmerzensgeldforderungen ohne materiellen Schaden,
- die Pseudonymisierung von Daten nach dem Urteil des EuGH vom 04.09.2025,
- Fragen die Künstliche Intelligenz betreffend,
- den Umgang mit Führungszeugnissen,
- die Überarbeitung der Muster für Auftragsverarbeitungen,
- Datenschutzhinweise für Beschäftigte,
- einzelne Verarbeitungstätigkeiten und IT-Systeme,
- notwendige Joint Controller Vereinbarungen,
- Fragen hinsichtlich der SAP–Harmonisierung,
- Prüfung der Datenverarbeitung durch die Baden-Badener Pensionskasse,
- weitere informationstechnische Harmonisierungen,
- Nutzungsmessungen im Allgemeinen und hbbTV-Nutzungsmessungen,
- Auskunftsersuchen,
- Erarbeitung neuer, harmonisierter Datenschutzschulungen.

Strukturell hat sich der AKDSB intern neu gegliedert, um die veränderten Strukturen im öffentlich-rechtlichen Rundfunk und die Digitalisierungsprozesse besser begleiten zu können. So gab es beispielsweise ein entsprechendes Erfordernis, um die Plattformstrategie der ARD besser beraten zu können.

II. Tätigkeitsschwerpunkte bezüglich Datenverarbeitungen im NDR

In einem zunehmend digitalisierten Umfeld kommt es zwangsläufig zu einer Verarbeitung personenbezogener Daten. Selbst wenn die originäre Tätigkeit nicht in der Verarbeitung solcher Daten liegt, kommt es durch die Bedienung von digitalen Anwendungen zu einer Datenverarbeitung von zumindest Beschäftigtendaten. Die Tätigkeit bei der

- **Überwachung und Durchsetzung** datenschutzrechtlicher Vorgaben,
- der **Sensibilisierung** für datenschutzrechtliche Belange und
- **Beratung** hinsichtlich zu ergreifender Maßnahmen für den Schutz von betroffenen Personen

kennt daher nicht einen Tätigkeitsschwerpunkt, sondern mehrere. Denn die gesamte Tätigkeit wird aufgrund des regelmäßig vorhandenen Personenbezugs bei allen Vorgängen datenschutzrechtlich gespiegelt. In Kontinuität zu den vorherigen Berichten erfolgt die Darstellung erneut nach dieser Gliederung:

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

1. Zur Umsetzung der DSGVO

Es gibt eine Reihe von datenschutzrechtlichen Vorgaben, die stets zu beachten sind. Die zentralen Grundsätze enthält Art. 5 DSGVO. Danach dürfen personenbezogene Daten nur

- rechtmäßig, transparent und nach dem Grundsatz von Treu und Glauben,
- für festgelegte, eindeutige und legitime Zwecke,
- nach den Grundsätzen der Sparsamkeit, Richtigkeit, Aktualität Speicherbegrenzung und Sicherheit („Integrität und Vertraulichkeit“)

verarbeitet werden.

Zur Umsetzung dieser und weiterer Vorgaben wurde eine Checkliste erarbeitet und zur Verfügung gestellt. Diese wird fortlaufend an die aktuellen Entwicklungen und an die Rechtsprechung angepasst. Einzelfallberatungen macht dies zwar nicht obsolet. Es ist jedoch eine Erinnerung und Hilfestellung bei der praktischen Tätigkeit des Verantwortlichen.

2. Programm und Programmverbreitung

Die digitale Programmverbreitung löst regelmäßig einen Datentransfer aus, der einen Personenbezug haben kann. Folglich gab es entsprechenden Beratungsbedarf und Anfragen dazu.

a) Datenschutzerklärungen und Informationspflichten

Anfang Dezember 2025 wurde eine neue Version der **Tagesschau-App** veröffentlicht. Damit war auch eine Revision der entsprechenden Datenschutzerklärung erforderlich. Noch in Klärung befindet sich eine diesbezügliche Anfrage zu „Emotionen". Denn es besteht die Möglichkeit, zu den Nachrichten ein **Stimmungsbild** zu erzeugen:

„Stimmungsbilder zu jeder Meldung
Durch die Abstimmung entsteht unter den täglich Millionen Nutzenden der *tagesschau*-App ein differenziertes Stimmungsbild, das bei jeder Meldung ab einer Beteiligung von 500 Nutzenden direkt im Abstimmungsfenster angezeigt werden kann. Der einzelne Nutzende sieht so, wie eine bestimmte Meldung auf andere Nutzende wirkt. Die Beteiligung an der Abstimmung ist freiwillig und erfolgt völlig anonym.

Warum interessiert sich die tagesschau für meine Gefühle?
Wichtiger Treiber dieser Neuentwicklung ist das Phänomen der Nachrichtenmüdigkeit, das in wissenschaftlichen Untersuchungen und Befragungen des Publikums häufig beschrieben wird. Gemeint ist damit, dass viele der aktuellen Nachrichten negative Folgen bei Nutzenden haben können, berichtet wird über Stress, Erschöpfung oder Depression" (https://www.tagesschau.de/app#:~:text=Warum%20interessiert%20sich%2

0die%20tagesschau,%C3%BCber%20Stress%2C%20Ersch%C3%B6pfung%20oder%20Depression).

Diesbezüglich wird noch untersucht, welche Datenströme die Teilnahme an der Herstellung eines solchen Stimmungsbildes hervorruft.

Aufgrund der digitalen Angeboten zukommenden Dynamik wurden und werden zudem derzeit und fortlaufend die Neufassungen der weiteren Datenschutzerklärungen der übrigen vom NDR verantworteten Telemedienangebote beraten.

b) Externe Anfragen zu Angeboten und Programmtätigkeiten des NDR

Eine Reihe von Anfragen gab es hinsichtlich der Angebote und der diesbezüglich vor- und nachgelagerten Tätigkeiten des NDR zu bearbeiten. Die Zuschriften betrafen u. a., wie zuvor auch,

- Datenschutzbestimmungen,
- technische Funktionalitäten,
- Drittplattformen und – neben weiteren Belangen – vermehrt
- redaktionelle Inhalte.

In diversen Anfragen und Löschbegehren wurde vorgetragen, dass Personen oder personenbezogene Daten in den Angeboten zu sehen seien, ohne dass die datenschutzrechtlich erforderlichen Voraussetzungen eingehalten seien.

Regelmäßig war darauf zu verweisen, dass für die journalistische Tätigkeit **Bereichsausnahmen von datenschutzrechtlichen Vorgaben** existieren. Datenschutzrechtliche Einwilligungserfordernisse und die sogenannten Betroffenenrechte (Widerruf, Löschung etc.) gelten nach wie vor nur nach Maßgabe des Kunsturhebergesetzes (KUG) und gemäß dem Medienstaatsvertrag. D. h., es gelten lediglich die allgemeinen Einwilligungserfordernisse aus dem Persönlichkeitsrecht für Filmausnahmen, die seit jeher gelten (§§ 22, 23 KUG). Dass das Kunsturhebergesetz im journalistischen Bereich weiterhin Anwendung findet, hatte der BGH bereits mit Urteil vom 7. Juli 2020 (Az.: VI ZR 246/19) festgestellt. Die bisherige ist mithin auch die aktuelle Rechtslage:

§ 22 S. 1 KUG
Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

§ 23 Abs. 1 KUG
Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:
1. Bildnisse aus dem Bereich der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben.

Wird eine Einwilligung widerrufen, braucht es dafür besondere Gründe, weil das Programmvermögen stark beeinträchtigt werden könnte. Daher hat z. B. das OLG Koblenz entschieden (Beschluss vom 31.07.2024, Az. 4 U 238/23), dass ein solcher Widerruf einer Einwilligung zur Veröffentlichung von Videoaufnahmen zwar grundsätzlich 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.

Bei den eingegangenen Zuschriften handelte es sich in der Regel um **aufmerksame und hilfreiche Hinweise**. Dies gilt auch für die Fälle, die als formale Beschwerde eingereicht wurden. Gelegentlich wurden diese für andere Personen eingereicht. Das Beschwerderecht des Art. 77 DSGVO steht allerdings nur Personen zu, die von einer Datenverarbeitung selbst betroffen sind („Jede betroffene Person hat …“). Sofern daher keine eigene Betroffenheit festzustellen war, hatte die Beschwerde formal keinen Erfolg. Gleichwohl konnte in der jeweiligen Sache geprüft und seitens des NDR gehandelt werden, womit die Angelegenheiten ganz überwiegend zielführend waren.

Gelegentlich führt auch die **Einbettung von Inhalten Dritter** in die Angebote des NDR zu Nachfragen. Das Einbetten fremder Inhalte (Embedding) in eigene Websites oder Apps entspricht einer üblichen Praxis bei der Verbreitung digi-

taler Inhalte. Die Einbettung von externen Inhalten ist eine redaktionelle Entscheidung. Bei dieser sind aber auch datenschutzrechtliche Anforderungen zu beachten, da sichergestellt sein muss, dass personenbezogene Daten erst dann an den Drittanbieter übermittelt werden, wenn sich die Nutzenden aktiv dafür entschieden haben. Bei der regelmäßig eingesetzten sogenannten „Zwei-Klick-Lösung“ sind die fremden Inhalte bei Aufruf der Angebote des öffentlich-rechtlichen Rundfunks zunächst inaktiv. Erst nach der Aktivierung beginnt die Datenübertragung, was datenschutzrechtlich als konform anzusehen ist.

c) Anfragen von Redaktionen

Auch wenn das redaktionelle Arbeiten in Teilen von datenschutzrechtlichen Vorgaben entbunden ist, stellen sich eine Reihe von Fragen aus dem redaktionellen Umfeld. Diese betrafen

- die Beschaffung von (KI-) Tools für die redaktionelle Arbeit,
- Anforderungen an Verarbeitungen von Publikumsdaten,
- Fragebögen für das Studiopublikum,
- Datenerhebungen für Akkreditierungszwecke,
- Datenschutzfragen zum ESC (Vorentscheid),
- datenschutzrechtliche Vereinbarungen mit Externen,
- Anmeldungen und Registrierungen,
- den Datenschutz bei Gewinnspielen und Verlosungen,
- den Bezug von Newslettern,
- Anforderungen an Community-Management-Systeme,
- Datenschutzhinweise und weitere Anforderungen bei einzelnen Angebotsteilen.

Wie bereits im Jahr zuvor, ist das Interesse und damit der Bedarf an der Nutzung von Künstlicher Intelligenz gewachsen. KI ist dabei nicht nur ein Arbeitsmittel, sondern häufig zugleich auch ein Recherchetool. Ausführungen dazu folgen unter dem gesonderten Punkt „Künstliche Intelligenz“. Eindeutig hat sich der Einsatz von KI im NDR zu einem gewichtigen Schwerpunkt verlagert.

3. Beschwerden: Beitragseinzug und weitere Themen

Fragen zum Rundfunkteilnehmerdatenschutz gibt es seit jeher in der Aufsichtstätigkeit. Regelmäßig werden sie in Form von Beschwerden eingereicht. Das Aufkommen ist konstant hoch. Vielfach lautet der Vortrag in den diesbezüglichen Beschwerdeschriften, dass die vom Beitragsservice erteilten Auskünfte nicht den gesetzlichen Vorgaben entsprächen und damit insbesondere unvollständig seien. Verkannt wird dabei regelmäßig, dass der in Art. 15 DSGVO geregelte Auskunftsanspruch spezialgesetzlich durch den Rundfunkbeitragsstaatsvertrag modifiziert wurde. Der Auskunftsanspruch hinsichtlich der zum Zwecke des Rundfunkbeitragseinzugs verarbeiteten personenbezogenen Daten richtet sich allein nach § 11 Abs. 8 Rundfunkbeitragsstaatsvertrag (RBStV). Die 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 ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, sind vom datenschutzrechtlichen Auskunftsanspruch nicht umfasst.“

Gemäß diesen Anforderungen erfolgen die vom Beitragsservice erteilten Auskünfte. Sie sind daher als vollständig anzusehen. Die öffentliche Verwaltung, zu der die Rundfunkanstalten bzw. der in ihrem Auftrag handelnde Beitragsservice zu zählen sind, hat 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. Da die genannte Vorschrift mangels entsprechender Entscheidungen mithin Geltung hat, muss vom NDR keine anderweitige Auskunft erteilt werden. Daher umfasst dieser Auskunftsanspruch auch nicht das Recht, Kopien von Schriftstücken zu erhalten. Das datenschutzrechtliche Auskunftsrecht des Rundfunkbeitragsstaatsvertrages ist kein Recht auf Akteneinsicht und kein Recht auf Übersendung von Kopien aller zu einer Person verarbeiteten Schriftstücke. Der Verantwortliche hat eine strukturierte Zusammenfassung der personenbezogenen Daten zur Verfügung zu stellen, nicht aber eine Übersendung aller Dokumente in Kopie vorzunehmen.

Die entsprechend vorgenommenen, rund 30 Prüfungen, konnten daher keine Verletzungen von datenschutzrechtlichen Vorgaben erkennen. Eine dieser Prüfungen war auch Gegenstand eines Gerichtsverfahrens. **Die Rechtmäßigkeit der Art und Weise der Erteilung einer Auskunft nach § 11 Abs. 8 RBStV hat das Schleswig-Holsteinische Verwaltungsgericht** mit Urteil vom 25.09.2025 bestätigt (Az. 6 A 70/25).

Damit hat das Gericht zugleich auch die Annahme des Gesetzgebers bestätigt, die der Begründung zum 21. Rundfunkänderungsstaatsvertrag zu entnehmen ist:

„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 Mitgliedstaaten 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 (vgl. § 1).

Im Ergebnis kann an den bislang geltenden Regelungen im Wesentlichen festgehalten werden. Für die Beitragsschuldner bestehen auch weiterhin nur die im Rundfunkbeitragsstaatsvertrag geregelten Informations- und Auskunftsansprüche."

Regelmäßig war auf diese und weitere Fragen bezüglich des Beitragseinzugs einzugehen.

Im Jahr 2024 hat der Beitragsservice in Köln **insgesamt 25.925 Datenauskünfte versandt, davon 4.533 für den NDR**. Im Berichtsjahr 2025 waren es weitaus mehr. **41.068 Datenauskünfte wurden erteilt, davon 6.473 für den NDR.** Der NDR hat 64 Auskunftsanträge erhalten (im Jahr im Jahr 2024 waren es 17). Zahlreiche Beschwerden wurde diesbezüglich eingereicht.

Beschwerden wurden auch zu anderen Belangen eingereicht. Hinsichtlich der Anzahl war der Beitragseinzug aber der Schwerpunkt. Erwähnt werden sei an dieser Stelle noch eine Beschwerde über die **Videoüberwachungen** des NDR. An einigen Stellen auf den Betriebsgeländen des NDR sind Videokameras installiert. In einer diesbezüglichen Beschwerde wurde vorgetragen, dass die Videoüberwachungen nicht hinreichend ausgewiesen seien bzw. auch Teile des öffentlichen Raumes umfassten. Auch wenn es aus formalen Gründen an einer Beschwerdebefugnis mangelte, wurde der Vorgang zum Anlass genommen, die Videoüberwachungen zu prüfen. Das Ergebnis war zufriedenstellend. Denn es war nicht festzustellen, dass öffentliche Flächen von den Kameras erfasst werden. Auch sind die Orte, an denen eine Überwachung erfolgt, mit großen und gut sichtbaren Schildern mit Kamerasymbolen ausgewiesen. Dazu liegen Informationsblätter mit weiteren Hinweisen in den Pförtnerlogen und an allen Empfangsbereichen aus. Zudem ist der NDR nicht immer Eigentümer von Gebäuden, in denen er seine Tätigkeiten verrichtet. So gibt es beispielsweise an einigen Standorten angemietete Studios. Dort findet auch der NDR Kameras vor, die von den Eigentümern installiert wurden. Auf etwaige Daten und deren Verarbeitung aufgrund einer Videoüberwachung hat der NDR keinen Zugriff und keinen Einfluss und ist daher nicht Verantwortlicher im Sinne der DSGVO. Ergänzend weist der NDR auch online unter https://www.ndr.de/der_ndr/kontakt/Wegweiser-zum-Norddeutschen-Rundfunk,wegweiser6.html auf die Videoüberwachung hin.

4. Beschäftigtendatenschutz

Die Verarbeitung von Personaldaten ist unerlässlich für die Durchführung von Arbeitsverhältnissen. Auch dabei gelten die oben genannten Grundsätze des Art. 5 DSGVO. Damit darüber hinreichend Transparenz hergestellt wird, wurde ein Vorschlag unterbreitet, wie alle Beschäftigten über die diesbezüglichen Verarbeitungstätigkeiten informiert werden. Zudem gab es eine Vielzahl von Maßnahmen und Verarbeitungstätigkeiten, die darüber hinaus diesbezüglich begleitet und beraten wurden.

a) Schulungen

Es wurde bereits kurz erwähnt, dass der AKDSB ein neues digitales Schulungskonzept zum Datenschutz für Beschäftigte erarbeitet hat. Diese Schulung soll allen Beschäftigten der Rundfunkanstalten digital zur Verfügung gestellt werden. Es ersetzt die klassischen Schulungen nur teilweise, weil es sich um eine Vermittlung von Grundlagen handelt. Auch zukünftig soll es ergänzend Termine geben, in denen bereichsspezifisch und konkret auf datenschutzrechtliche Belange eingegangen wird. Solche Termine gab es auch im Berichtsjahr, etwa mit den Aufnahmeleitungen mit dem Schwerpunkt Akkreditierungen, und den Personalvertretungen sowie den neuen Auszubildenden und Volontär*innen. In Aussicht genommen wurde zudem, die aktuellen Schulungskonzepte für Präsenztermine zu überarbeiten. Denn es hat sich in den vergangenen Jahren herausgestellt, dass die Schulungsinhalte zugenommen haben, weshalb über die Form und Schwerpunktsetzung nachgedacht werden muss. Die anwachsende und strenge Rechtsprechung zum Datenschutz erfordert dies, aber auch der alltäglich gewordene Einsatz von Anwendungen Künstlicher Intelligenz.

An dieser Stelle sei hervorgehoben, dass der im Jahr entwickelte **KI-Führerschein** als Erfolg bezeichnet werden kann. Weitere Rundfunkanstalten haben diesen für ihre Beschäftigten übernommen. Im NDR ist der Führerschein verpflichtend zu absolvieren, bevor KI-Anwendungen genutzt werden.

Neben den o. g. Schulungen gab es eine Reihe von Terminen, in denen spezifische Datenschutzfragen in unterschiedlichen Bereichen des NDR erörtert

wurden. Um diesen Austausch zu intensivieren und zu verstetigen, wird ein Vorschlag unterbreitet, der eine Struktur im NDR schaffen soll, in der sogenannte Datenschutzkoordinator*innen tätig werden. Andere Rundfunkanstalten haben derartige Funktionen bereits geschaffen. Diese Koordinator*innen sind – ohne formales Amt – Ansprechpartner*innen der Datenschutzbeauftragten in „sensiblen" Bereichen und treten in einen Regelaustausch mit diesem. Dies soll das Datenschutzniveau erhöhen und für mehr Awareness sorgen. Geeignete Bereiche dafür könnten beispielsweise solche sein, die sich mit Personalangelegenheiten befassen, aber auch die Medienforschung und Personen, die maßgeblich den Einsatz von KI steuern.

b) Umfragen

Der NDR führt eine Reihe von Umfragen unter Beschäftigten durch. Zur Wahrung der Anonymität und Einhaltung weiterer Voraussetzungen wird häufig der Verfasser dieses Berichts zu Rate gezogen. So etwa bei der „**Umfrage zu Null Toleranz bei Sexismus am Arbeitsplatz**". Aber auch bei internen Wahlvorgängen ist datenschutzrechtliche Expertise gefragt.

Leider kam es aber auch zu einem Vorfall, bei dem fast keine datenschutzrechtlichen Vorgaben eingehalten wurden: In einem Bereich wurde eine telefonische Umfrage unter Beschäftigten durchgeführt. Beauftragt wurde dafür ein externer Dienstleister. Es mangelte bedauerlicherweise an einer formal korrekten Beauftragung des Dienstleisters, auch die gebotene Transparenz wurde zuvor nicht hergestellt. Nur weil die Erkenntnis über die mangelnde Datenschutzkonformität rasch und von selbst gewachsen war und eine Entschuldigung ausgesprochen wurde, konnte von einer aufsichtsrechtlichen Maßnahme abgesehen werden.

In diesen Angelegenheiten gilt stets:

1. Keine Pflicht zur Teilnahme/Freiwilligkeit

Eine Pflicht zur Teilnahme an derartigen Umfragen besteht nicht, sie sind freiwillig. Es darf auch nicht der Eindruck entstehen, dass eine Teilnahme erforderlich ist bzw. dass sich Nachteile ergeben, wenn keine Teilnahme erfolgt. Jegliche Ausübung von Druck ist nicht gestattet.

2. Anonymität

Unabhängig davon, ob der Verantwortliche (NDR) Umfragen selbst durchführt oder einen Dienstleister beauftragt, müssen Umfragen so gestaltet sein, dass etwaige Rückschlüsse auf Beschäftigte nicht möglich sind. Die Erhebung von personenbezogenen oder -beziehbaren Daten ist auszuschließen.

3. Transparenz

Bei der Erhebung/Verarbeitung personenbezogener Daten gelten Transparenzverpflichtungen gemäß Art. 13 DSGVO. Diese Vorschrift lautet auszugsweise:

„Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- [...];
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- [...].

Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Wi-

derspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- [...];
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;“

Im Falle einer telefonischen Umfrage können diese Angaben schwerlich mündlich übermittelt werden. Eine schriftliche Vorab-Information an die Mitarbeitenden, in der erläutert wird, warum und wie die Daten erhoben, verarbeitet und gespeichert werden, ist daher erforderlich. In „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ (Art. 12 DSGVO) sind diese Informationen – auch über die Speicherdauer – zu erteilen. Gleiches gilt auch für die Rechte der Mitarbeitenden: Über das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und das Recht auf Beschwerde ist zu informieren.

4. Formalitäten

Werden externe Personen oder Unternehmen mit einer Umfrage beauftragt, ist gelegentlich zur Durchführung einer Umfrage die Weitergabe von personenbezogenen oder -beziehbaren Daten erforderlich (das können Namen, E-Mail-Adressen oder andere Erreichbarkeiten wie Durchwahlnummern sein).

Wird eine externe private oder juristische Person mit der Durchführung beauftragt, ist neben dem Hauptvertrag eine Auftragsverarbeitungsvereinbarung zu schließen (AVV). Eine AVV hat gemäß Art. 28 DSGVO bestimmte Inhaltsvorgaben. Art. 28 Abs. 3 DSGVO lautet auszugsweise: „Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.“

5. Weitere Anforderungen

Eine vollständig anonyme Umfrage ist wünschenswert, gelegentlich in der Praxis (am Telefon) aber nur schwer umzusetzen. Daher gilt:

- Bei der Erhebung personenbezogener Daten ist die Einholung von informierten und freiwilligen Einwilligungen erforderlich. Das Vorliegen dieser Einwilligungen ist zu dokumentieren.
- Der Grundsatz der Datenminimierung gebietet, dass nur die für den Zweck der Umfrage notwendigen Daten erhoben werden.
- Der Verantwortliche und sein Auftragnehmer müssen gewährleisten, dass die Informationen durch angemessene technische und organisatorische Maßnahmen sicher verarbeitet werden.

Diese breite Darstellung erfolgt in der Hoffnung, dass diese Anforderungen künftig vollständig umgesetzt werden.

c) Weitere Beratungen, Personalentwicklung

Die NDR-interne Digitalisierung ging mit einem regen Beratungsbedarf einher, weil auch Personaldaten sehr vertraulich zu behandeln sind. Beratungsgegenstände waren beispielsweise

- die Einführung der digitalen Entgeltabrechnung,
- Arbeitszeiterfassungen,
- der Umgang mit Führungszeugnissen,
- die Umsetzung des Hinweisgeberschutzgesetzes,
- die datenschutzkonforme Umsetzung von Embargo-Richtlinien,
- digitale Signaturen,
- Verleihstationen für Produktionsausstattungen,
- Schutzkonzepte für Mitarbeitende,
- Reisekostenabrechnungen,
- Seminarmanagementsysteme,
- Datenschutzfragen bei der Wahl der Gleichstellungsbeauftragten,
- ein sog. Talentmanagement.

Der Einsatz eines **Talentmanagement-Tools** unterliegt besonderen Anforderungen. Denn solche Anwendungen sollen Leistungs- und „Performance-“ Daten von Beschäftigten erfassen. Hintergrund ist eine intendierte Personalplanung, mit der registriert wird, ob einzelne Beschäftigte für bestimmte Positi-

onen oder Projekte geeignet sind. Entscheidend für den Einsatz eines solchen Tools wird sein, inwieweit eine solche Datenverarbeitung der Durchführung von Beschäftigungsverhältnissen dient. Dazu wird es auf die im Einzelnen verarbeiteten Datenkategorien ankommen. Der NDR hat das Projekt noch nicht abgeschlossen. Im Detail sind noch diese Fragen zu klären:

1. Welche Kategorien von Daten werden genau verarbeitet?
2. Gebot der Datenminimierung: Nicht erforderliche Daten dürfen nicht erfasst werden. Eine genaue Beschreibung der Kategorien und der Zwecke ist erforderlich.
3. Auf welcher Rechtsgrundlage soll die Verarbeitung der Daten stattfinden?
4. Wo werden die Daten verarbeitet? Es darf keine geheime Verarbeitung stattfinden (Transparenzgebot. Personenbezogene Daten dürfen nicht treuwidrig verarbeitet werden, d. h. Betroffene müssen hinreichende Kenntnis von der Verarbeitung und Art und Umfang der Verarbeitung erlangen können.).
5. Wie werden die Rechte der Personen gewahrt, deren Daten verarbeitet werden (Auskunft, Löschung, Widerruf etc.)
6. Wie und wann werden die Daten gelöscht (auch von einzelnen Datensätzen)?
7. Wer hat Zugriff auf die Daten (Berechtigungskonzept)?
8. Wo findet die Speicherung der Daten statt? Bei einem Dienstleister? In einer Cloud? In jedem Fall gilt: Die Sicherheit der Daten ist zu gewährleisten. (Personenbezogene) Daten sind gegen unbefugte Einsichtnahme oder Entwendung zu schützen.
9. Wie werden die Daten gesichert?

d) Desk-Sharing und Umzüge

Die fortwährenden Digitalisierungsprozesse haben auch Auswirkungen auf die Gestaltung von Arbeitsplätzen. Dies gilt nicht nur mit Blick auf die Ausstattung des Personals mit Endgeräten, sondern auch hinsichtlich der vorgehaltenen Arbeitsplätze. Räumlichkeiten sind nach wie vor so zu gestalten, dass nur befugte Mitarbeitende dort Zugang haben. Kontakte mit Anfragenden müssen vertraulich behandelt werden können. Besprechungen von einzelnen, sensiblen Einheiten müssen gegebenenfalls in speziellen Räumlich-

keiten stattfinden, damit nur die jeweils mit den spezifischen Angelegenheiten befassten Beschäftigten Zugang zu den Informationen haben. Und auch Telefonate und Gespräche müssen in einer Umgebung stattfinden können, die entsprechend geschützt ist. Sollte dies ein einzelner Arbeitsplatz nicht gewährleisten können, sind die bereits erörterten Telefonkabinen bzw. Telefonräume einzurichten. Auch auf die Einhaltung der übrigen Standards (Monitore mit Sichtschutz, Verschluss von analogen Unterlagen) ist zu achten.

5. Künstliche Intelligenz

Der Umgang mit Anwendungen Künstlicher Intelligenz wurde zunehmend ausdifferenziert. Der „KI-Führerschein“ wurde bereits angesprochen. Zudem hat der NDR eine Reihe weiterer Vorgaben und Leitlinien erlassen, um Potenziale zu schöpfen und Risiken zu minimieren.

Die aus der Anwendung von KI resultierenden Risiken sind groß. Es sollen an dieser Stelle nicht alle Risiken aufgeführt werden, sondern nur so viel:

KI-Anwendungen sind darauf trainiert, Antworten zu geben. Weiß ein KI-System keine Antwort, so erfindet es diese. Genannt wird dies in diesem Zusammenhang „**Halluzinieren**“. In einer Studie der Europäischen Rundfunkunion (EBU) wurde ermittelt, dass KI-Chatbots „gerne“ Informationen erfinden oder falsche Quellen angeben: „ChatGPT, Gemini und andere Chatbots erfinden bis zu 40 Prozent ihrer Antworten und stellen sie als Fakten dar“ (https://www.tagesschau.de/wissen/technologie/kuenstliche-intelligenz-fakten-100.html). Die Studie ist unter https://www.ebu.ch/Report/MIS-BBC/NI_AI_2025.pdf abrufbar.

Weiteres Risiko: Die **Eingabe interner oder vertraulicher Informationen** in derartige Systeme führt dazu, dass diese Informationen auch Dritten zugänglich gemacht werden können, etwa durch das Trainieren der Systeme mit diesen Daten. Daraus können Verletzungen des informationellen Selbstbestimmungsrechts folgen, aber auch unbeabsichtigte Veröffentlichungen von Betriebsgeheimnissen und daraus resultierende Kosten, vermehrte Cyberangriffe und Reputationsverluste.

Es stehen derzeit nur wenige technische Maßnahmen zur Verfügung, um diese Risiken einzudämmen. Daher ist bei der Auswahl der Anwendungen besondere Achtsamkeit geboten. Zudem sind organisatorische Maßnahmen zu ergreifen. Im Bericht für das Jahr 2024 wurde auf das Erfordernis der Klassifikation von Informationen hingewiesen. Durch die Einstufung von Informationen in einen jeweiligen **Grad der Vertraulichkeit** und eine entsprechende Schutzklasse können Risiken zumindest minimiert werden. Die Informationsklassen

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

sind – nicht nur bei dem Einsatz von KI – mitzudenken und anzuwenden.

Vor einem Jahr wurde an dieser Stelle formuliert: **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." Mittlerweile hat sich die Klassifikation gut verbreitet und wird vermehrt verstanden und umgesetzt. Ein diesbezüglicher **technischer Prozess** sollte allerdings begleitend implementiert werden, um die tägliche Arbeit zu erleichtern. Denn rund 40 KI-Anwendungen sind in der Erprobung und die wenigstens können ohne weiteres vollumfänglich (datenschutzkonform) eingesetzt werden. Dies führte zu einem stark erhöhten Arbeitsaufkommen und Beratungsbedarf.

Aber auch im Falle künftiger technischer Mittel zur Klassifikation von Informationen ist und bleibt der „**Human-in-the-loop Ansatz**" entscheidend: Anwendungen Künstlicher Intelligenz dürfen nicht selbst entscheiden und müssen menschlich kontrolliert werden. KI arbeitet oft nicht vertraulich (s. o.) und bringt oft auch keine vertrauenswürdigen Ergebnisse hervor. Ob eine KI halluziniert, muss von Menschen überprüft werden. Gleiches gilt hinsichtlich der Eignung der Verarbeitung von Inhalten durch eine KI.

6. Weitere Beratungen und Prüfungen

Neben den genannten Beratungen zu Projekten und Anwendungen gab es eine Vielzahl von datenschutzrechtlichen Beratungen und Einschätzungen aus allen Bereichen des NDR. Fast **150 Begutachtungen** von IT-Anwendungen und Prototypen wurden aus datenschutzrechtlicher Perspektive vorgenommen. Dabei ging es etwa um die Erneuerung von Audioregien, Investitionsdatenbanken, Feedbacktools, Redaktionswerkzeugen, Berechtigungskonzepten, Verzeichnisdiensten, mobilen Datenzugängen, Grafiksystemen, Cloud-Diensten, Löschkonzepten, Anonymisierungsanforderungen und Maßnahmen zur Erhaltung und Stärkung der IT-Sicherheit.

F. Anfragen nach dem Informationszugang

Im Jahr 2025 wurden rund 22 Anfragen auf Informationszugang an den NDR gerichtet. Damit hat sich die Zahl im Vergleich zum Vorjahr verringert. Dies gilt auch für die Anrufung des Rundfunkdatenschutzbeauftragten als Beschwerdestelle. Auch wenn die Anzahl der Anfragen abgenommen hat, war gleichwohl der Befassungsaufwand größer. Denn nicht immer gelang es, anfragende Personen vom ermittelten Prüfergebnis zu überzeugen. Ähnlich wie bei Beschwerdeverfahren entwickelte sich nicht selten eine langwierige Korrespondenz. In dieser galt es zu vermitteln, dass die vom Gesetzgeber geschaffenen Bereichsausnahmen in manchen Fällen dazu führen, dass der Verantwortliche (NDR) keine Auskunft zu erteilen hat:

Von dem Anspruch auf Informationszugang sind Informationen ausgeschlossen, über die der NDR zu journalistisch-redaktionellen Zwecken verfügt. Informationen zu Produktionen und deren Kalkulationen sind beispielsweise ebenfalls als solche einzuordnen, weil diese für die Erstellung (und Verbreitung) eines journalistisch-redaktionellen Erzeugnisses erforderlich sind und allein zu diesem Zweck vorgehalten werden. Das sogenannte Medienprivileg für die journalistisch-redaktionelle Arbeit greift analog auch hier und bildet damit die verfassungsrechtlich gebotene einfachgesetzliche Lösung des grundrechtlichen Konflikts zwischen Datenschutz, Informations- und Rundfunkfreiheit. Im NDR Staatsvertrag hat dies seinen Niederschlag in § 47 Abs. 1 S. 2 NDR Staatsvertrag gefunden.

G. Ende

Dies ist der letzte Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten des NDR. Der schon gelegentlich erwähnte Reformstaatsvertrag/7. Medienänderungsstaatsvertrag sieht in § 31 j eine*n gemeinsame*n Rundfunkdatenschutzbeauftragte*n für alle Rundfunkanstalten mit Ausnahme der Deutschen Welle vor. Damit war die gemäß § 44 NDR Staatsvertrag eingesetzte Aufsichtsbehörde aufzulösen. **Das Amt bestand seit dem 25. Mai 2018 und damit fast 8 Jahre**. Insgesamt kann festgehalten werden, dass es gelungen ist, die Vorgaben der DSGVO umzusetzen und die dafür notwendigen Strukturen zu schaffen. Auch wenn die Aufsichtstätigkeit anderweitig vorgenommen wird, bleiben die Herausforderungen bestehen. Nicht nur der eingangs kurz erwähnte § 26 a ReformStV, mit dem der Gesetzgeber eine „datengestützte Überprüfung der eigenen Leistung" der Rundfunkanstalten einführt, wird datenschutzrechtlich für mehr Befassungsaufwand sorgen. Auch die europäische Neuordnung des digitalen Rechtsrahmens und die zunehmenden tatsächlichen Entwicklungen, maßgeblich im Bereich der Künstlichen Intelligenz, werden diesbezüglich Aufwand erzeugen. Um den vielfältigen Risiken zu begegnen, bedarf es insbesondere auch eines Verständnisses für diese Belange. Eine einschlägige Studie zu den Haltungen zum Datenschutz wurde erwähnt. Danach gibt es zumindest Hoffnung, dass das Thema mehr Aufmerksamkeit erfährt. „Gut Ding will Weile haben", heißt es oft. Und wie so oft bietet sich auch hier eine Parallele zum Straßenverkehr an: Vor 50 Jahren, am 1. Januar 1976, wurde in Deutschland die Anschnallpflicht für Fahrer- und Beifahrer*innen eingeführt. Die sogenannten „Gurtmuffel" ignorierten dies zunächst gern. Aber **8 Jahre** später, 1984, wurde das Nichtanschnallen mit einem Bußgeld belegt, und die Pflicht etabliert sich, auch weil das **Risiko bekannt und die Maßnahme als wirksam angesehen wurde**. Eine solche Entwicklung hat auch der Datenschutz verdient. Zum Abschluss noch ein entsprechender Slop: