

# NORDDEUTSCHER RUNDFUNK

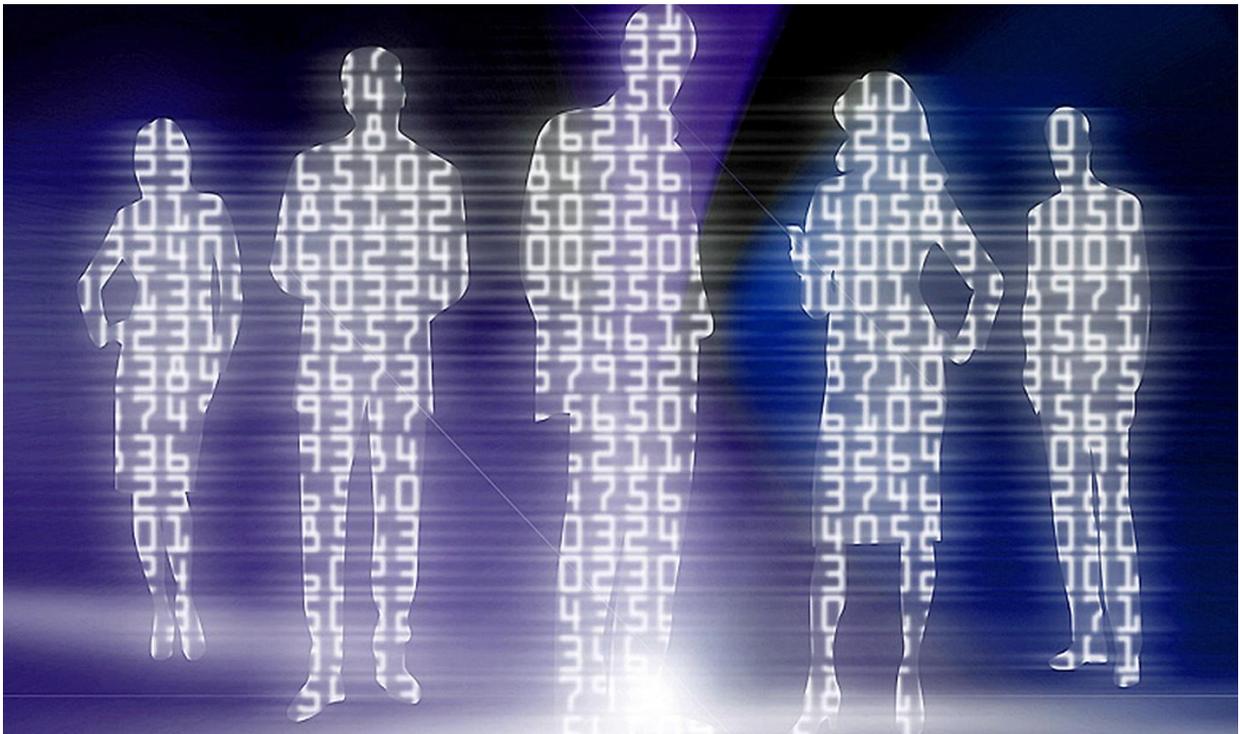
## Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten des NDR

---

für das Berichtsjahr 2022

Dr. Heiko Neuhoff

Hamburg im Januar 2023



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 2022.

## **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.....	5
B.	Rechtsgrundlagen der Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR .....	6
C.	Personalien .....	7
D.	Wesentliche Entwicklungen im Berichtszeitraum (und zuvor) .....	7
I.	Gesetzgebung.....	9
1.	Hinweisgeberschutzgesetz.....	9
2.	Koalitionsverträge .....	10
3.	Entwicklungen auf Europäischer und internationaler Ebene.....	11
a)	Vom EU-US-Privacy Shield zum TADPF .....	11
b)	Weitere EU-Gesetzgebungen.....	12
4.	Bußgelder.....	12
II.	Rechtsprechung.....	13
1.	Zensus 2022.....	13
2.	Bundesverfassungsgericht zum Meldedatenabgleich .....	15
3.	Möglichkeiten des Datentransfers in die USA ohne Abkommen?.....	17
4.	Immaterieller Schadensersatz?.....	17
E.	Tätigkeiten des Rundfunkdatenschutzbeauftragten des NDR im Jahr 2022.....	18
I.	Organisationsstrukturen/Zusammenarbeit mit anderen Aufsichtsbehörden .....	18
1.	Die Rundfunkdatenschutzkonferenz (RDSK).....	19
a)	Organisation der RDSK.....	20
b)	Tätigkeitsschwerpunkte der RDSK.....	20
c)	Zusammenarbeit mit der Datenschutzkonferenz .....	21
2.	Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF, ORF, ARTE, DRadio und SRG SSR (AKDSB).....	22
II.	Tätigkeitsschwerpunkte bezüglich Datenverarbeitungen im NDR.....	25
1.	Zur Umsetzung der DSGVO .....	26
2.	Programm und Programmverbreitung .....	27
a)	Datenschutzerklärungen und Informationspflichten .....	27
b)	Informationsangebote der (Rundfunk-) Datenschutzbeauftragten .....	27
c)	Anfragen zu den Angeboten und Datenschutzerklärungen des NDR .....	28
d)	Anfragen von Redaktionen.....	33
3.	Rundfunkteilnehmerdatenschutz.....	34
4.	Beschäftigtendatenschutz .....	35

a)	Tarifvertrag hybride Arbeit.....	35
b)	IT-Rahmendienstvereinbarung.....	36
c)	Sichere elektronische Kommunikation von Personaldaten.....	37
d)	Auskunftsersuchen von beschäftigten Personen.....	37
e)	Löschung von Daten im Zusammenhang mit der Corona-Pandemie.....	38
f)	Schulungen.....	39
g)	Warnstreiks.....	40
h)	Umfragen unter Beschäftigten.....	40
i)	Elektronische Arbeitsunfähigkeitsbescheinigungen.....	42
5.	Weitere Beratungen und Prüfungen im NDR.....	42
a)	Organisations- und Strukturprojekte.....	43
b)	Datensicherheit.....	44
F.	Anfragen nach dem Informationszugang.....	45
G.	Fazit und Ausblick.....	46

## A. Einleitung

Mit diesem Bericht für das Jahr 2022 wird die Ankündigung umgesetzt, die Darstellung der Tätigkeiten zumindest etwas kürzer und straffer abzubilden, obgleich der Arbeitsumfang kontinuierlich zunimmt. Das Berichtsjahr ist – wie bereits das Jahr zuvor – geprägt durch intensive Prüfungen und Beratungen, die im Kern Digitalisierungsprozesse, Nutzungen von Cloud-Diensten, Auslagerungen von Datenverarbeitungen und die Datensicherheit betrafen. Handlungsbedarf gab es insbesondere bei

- neuen und veränderten digitalen Geschäftsvorgängen und Beschaffungen,
- der Überwachung und Durchsetzung datenschutzrechtlicher Vorgaben,
- der Bearbeitung von externen und internen und Beschwerden und
- der Vernetzung mit Aufsichtsbehörden und anderen Datenschutzbeauftragten.

Im durch globale Krisen gekennzeichneten Jahr 2022 war mit Blick auf den öffentlich-rechtlichen Rundfunk eine weitere Krise hinzugekommen. Nach zahlreichen Vorwürfen gegen die Intendantin des rbb und weitere Mitglieder der Geschäftsleitung gerieten auch der NDR und insbesondere die Landesfunkhäuser Schleswig-Holstein und Hamburg in den Fokus der Berichterstattung. Angestoßen wurde ein Prozess eines Kulturwandels zur Bewältigung der betrieblichen Klimakrise. Zudem wurde insgesamt im öffentlich-rechtlichen Rundfunk eine **programmliche und innere Neuausrichtung** vereinbart:

„Die Intendant\*innen [haben] beschlossen, die digitalen Programmangebote der ARD sowie den technologischen Ausbau der digitalen Infrastruktur zu priorisieren. Das bedeutet auch, dass im Linearen fokussiert werden muss, und die Landesrundfunkanstalten in noch mehr Bereichen kooperieren. Dieser Ausbau im Digitalen setzt voraus, dass die ARD Mittel umschichtet und Kraft sowie Ressourcen für den Umbau gewinnt – zum Beispiel durch engere Zusammenarbeit auf allen Ebenen“ (<https://www.ard.de/die-ard/wie-sie-uns-erreichen/ard-pressemitteilungen/2022/11-24-ARD-setzt-Prioritaet-im-Digitalen-und-beschliesst-einheitliche-Compliance-Standards-100>).

Außerdem haben die ARD-Anstalten zur Überwindung der Krise einen Leitfaden zu „ARD Compliance Standards“ beschlossen: <https://www.ard.de/ard/die-ard/Leitfaden-ARD-Compliance-Standards-100.pdf>. In diesem wird auf den Risikokatalog des Deutschen Instituts für Compliance e. V. Bezug genommen.



Quelle: Deutsches Institut für Compliance (<https://www.dico-ev.de/2016/08/30/dico-risikokatalog/>)

Auch wenn die Graphik keine Gewichtung der einzelnen Waben enthält, sind die Bausteine **Datenschutzrecht und IT-Sicherheit zu Recht an prominenter Stelle angesiedelt**. Datenschutzrecht/das Recht auf informationelle Selbstbestimmung ist das zentrale Grundrecht der Informationsgesellschaft, das von Anfang an in allen Geschäftsprozessen mitzudenken und zu implementieren ist.

## B. Rechtsgrundlagen der Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR

Die Grundlagen für die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR finden sich unverändert in der Datenschutzgrundverordnung (DSGVO) und in den §§ 43 bis 46 NDR Staatsvertrag. Auftrag und Aufgabe des Rundfunkdatenschutzbeauftragten als Aufsichtsbehörde nach Art. 51 DSGVO ist die Überwachung der Einhaltung der Datenschutzvorschriften bei der **gesamten Tätigkeit des NDR und seiner Beteiligungsunternehmen** im Sinne des § 42 Absatz 3 Satz 1 des Medienstaatsvertrages.

Weitere Aufgabe ist die Prüfung von Beschwerden nach § 47 NDR Staatsvertrag. Sofern Antragstellende der Auffassung sind, dass ein „Informationsanspruch zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass nur eine unzulängliche Antwort gegeben worden ist“, kann die\*der Rundfunkdatenschutzbeauftragte angerufen werden.

### C. Personalien

Seit dem 25. Mai 2022 läuft die zweite Amtszeit des Rundfunkdatenschutzbeauftragten des NDR für weitere vier Jahre. Personelle Änderungen hat es insgesamt nicht gegeben.

Mit Beginn des Jahres 2023 wird der Verfasser dieses Berichts aufgrund einer entsprechenden Wahl der stellvertretende Vorsitzende der Rundfunkdatenschutzkonferenz.

Für den Fall der Verhinderung des Rundfunkbeauftragten für den Datenschutz des MDR über einen Zeitraum von länger als 2 Monaten ist der Rundfunkdatenschutzbeauftragte des NDR sein Stellvertreter (Art. 2 Abs. 3 der Satzung über die Rundfunkbeauftragte für den Datenschutz des MDR). Ein solcher Fall trat jedoch nicht ein.

### D. Wesentliche Entwicklungen im Berichtszeitraum (und zuvor)

Das Bedürfnis nach Selbstbestimmung, die Abwehr von heimlichen Überwachungen, die Wahrung von Geheimnissen und der Schutz höchstpersönlicher Angelegenheiten reicht in der europäischen Rechtskultur weit zurück. Für unterschiedliche Zwecke wurden dafür – teils bis heute – eine Reihe von Schutzräumen geschaffen und Begriffen benutzt.

- Bereits um das Jahr 400 v. Chr. wurde der Hippokratische Eid eingeführt. Ärzt\*innen verpflichteten sich, Gesundheitsdaten nicht an Dritte herauszugeben. Diese **ärztliche Schweigepflicht** ist heute in entsprechenden Berufsordnungen festgelegt.
- Im Jahr 1215 wurde das Beichtgeheimnis auf dem Vierten Laterankonzil beschlossen.
- Die Allgemeine Preußische Postordnung regelte das Briefgeheimnis bereits ab dem 10. August 1712. Im Jahr 1851 wird das deutsche Steuergeheimnis beschlossen und die Weimarer Reichsverfassung von 1919 schützte in Art. 117 das **Fernsprech-, Brief- und Postgeheimnis**.

- Im Jahr 1890 wurde das **moderne Datenschutzrecht in Amerika** begründet. Die Juristen Louis D. Brandeis und Samuel D. Warren schufen mit ihrer Veröffentlichung „The Right to Privacy“ die Grundlage eines Rechts darauf, „in Ruhe gelassen zu werden“. Aufgrund gesellschaftlicher Entwicklungen (zunehmende Reichweiten von Zeitungen, vermehrter Einsatz der Fotografie) müsse auch die Privatheit und der Umgang mit persönlichen Angaben und Informationen neu bestimmt werden.
- Das sogenannte **Recht am eigenen Bild** – maßgeblich geregelt im Kunsturhebergesetz aus dem Jahr 1907 – ist noch heute Bestandteil der Rechtsordnung. Der damalige Gesetzgeber hatte eine Regelungslücke beseitigt, nachdem zwei Fotografen den verstorbenen Reichskanzler Otto von Bismarck in seinem Sterbezimmer abgelichtet hatten und die Bilder gewinnbringend veräußern wollten.
- In Hessen tritt am 13. Oktober **1970 das erste Datenschutzgesetz** überhaupt in Kraft. Ziel des Gesetzgebers waren persönlichkeitsrechtswahrende Regelungen für die automatisierte Informationsverarbeitung durch die Verwaltung.
- Vor fast 40 Jahren ergeht das **Volkszählungsurteil** des Bundesverfassungsgerichts. Das Gericht erfindet den Datenschutz nicht neu, erkennt aber ein umfassendes Recht auf informationelle Selbstbestimmung. Jede\*r hat mithin das Recht, grundsätzlich selbst über die Verwendung ihrer oder seiner Daten zu bestimmen.

Diese Auflistung ließe sich erheblich ergänzen und bis in das Jahr 2022 fortsetzen. Es geht hier indes nicht um Vollständigkeit, sondern um Bedeutung: Alle Regelungen sind bis heute aktuell und entfalten ihre Schutzwirkung. Eine Vielzahl weiterer Regelungen ist hinzugekommen. Datenschutzrecht/das Recht auf informationelle Selbstbestimmung ist das derzeit zentrale Grundrecht, denn:

„Die Digitalisierung verändert unsere Gesellschaft tiefgreifend. Neuartige datenbasierte Technologien können für das Leben des Einzelnen und das gesellschaftliche Zusammenleben Nutzen stiften, die Produktivität der Wirtschaft steigern, zu mehr Nachhaltigkeit und zu grundlegenden Fortschritten in der Wissenschaft beitragen. Gleichzeitig zeigen sich jedoch auch Risiken der Digitalisierung für grundlegende Rechte und Freiheiten. Es stellen sich damit zahlreiche ethische und rechtliche Fragen, in deren Mittelpunkt die gewünschte Rolle und die Gestaltung der neuen Technologien stehen. Wenn der digitale Wandel dem Wohl der gesamten Gesellschaft dienen soll, müssen sich Gesellschaft und Politik mit der Gestaltung datenbasierter Technologien einschließlich der Künstlichen Intelligenz (KI) befassen“ (Gutachten der Datenethikkommission der Bundesregierung, S. 12, abrufbar unter

[https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?\\_\\_blob=publicationFile&v=7](https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=7)).

## I. Gesetzgebung

Auf nationaler Ebene gab es eher wenig gesetzgeberische Tätigkeiten mit originär datenschutzrechtlichen Regelungen, soweit der öffentlich-rechtliche Rundfunk betroffen war.

### 1. Hinweisgeberschutzgesetz

Eigentlich hätte Deutschland die **EU-Whistleblower-Richtlinie** bis Ende Dezember 2021 in nationales Recht umsetzen müssen. Dies ist nicht geschehen, weshalb die EU-Kommission Anfang des Jahres 2022 ein förmliches Vertragsverletzungsverfahren gegen Deutschland (und weitere 22 Mitgliedstaaten) eingeleitet hat.

Immerhin gibt es nun einen Entwurf der Bundesregierung für ein „Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“. Damit ist das Gesetzgebungsverfahren eingeleitet worden für ein deutsches Hinweisgeberschutzgesetz. Ziel ist der Schutz von hinweisgebenden Personen:

„Mit einem neuen Gesetz zum Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG) soll deren bislang lückenhafter und unzureichender Schutz ausgebaut werden. Hinweisgeberinnen und Hinweisgeber leisten einen wichtigen Beitrag zur Aufdeckung und Ahndung von Missständen. Allerdings gab es in der Vergangenheit immer wieder Fälle, in denen sie infolge einer Meldung oder Offenlegung von Missständen benachteiligt wurden. Ziel dieses Gesetzentwurfes ist es, diese Benachteiligungen auszuschließen und Hinweisgeberinnen und Hinweisgebern Rechtssicherheit zu geben. Mit dem Gesetzentwurf soll das Ziel eines verbesserten Hinweisgeberschutzes mit den Interessen von Unternehmen und öffentlicher Verwaltung, die zum Ergreifen von Hinweisgeberschutzmaßnahmen verpflichtet werden, so in Einklang gebracht werden, dass bürokratische Belastungen handhabbar bleiben“

([https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE\\_Hinweisgeber-schutz.pdf;jsessionid=DB082139E5F9F60086432A238A83A22E.1\\_cid324?\\_\\_blob=publicationFile&v=2](https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Hinweisgeber-schutz.pdf;jsessionid=DB082139E5F9F60086432A238A83A22E.1_cid324?__blob=publicationFile&v=2)).

Das Gesetz sieht eine Pflicht zur Einrichtung einer internen Meldestelle in Unternehmen vor. Dazu zählen auch Rundfunkanstalten. Insbesondere der **Schutz der Vertraulichkeit der Identität der hinweisgebenden Person** soll gewährleistet werden. Anders als beim Beichtgeheimnis gibt es aber kein Verwertungsverbot der gewonnenen Erkenntnisse, da Missstände aufgedeckt und beseitigt werden sollen.

Im Jahr 2023 sollte das Gesetz in Kraft treten.

## 2. Koalitionsverträge

Der **Koalitionsvertrag 2021 – 2025 zwischen SPD, BÜNDNIS 90/DIE GRÜNEN UND FDP** benennt datenschutzrechtliche Vorhaben:

„Die Datenschutzgrundverordnung (DSGVO) ist eine gute internationale Standardsetzung. Zur besseren Durchsetzung und Kohärenz des Datenschutzes verstärken wir die europäische Zusammenarbeit, institutionalisieren die Datenschutzkonferenz im Bundesdatenschutzgesetz (BDSG) und wollen ihr rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen. Wir schaffen Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen. Wir setzen uns für eine schnelle Verabschiedung einer ambitionierten E-Privacy-Verordnung ein“

(<https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1>).

Die Umsetzung erfolgte bislang nicht, aber Datenschutz wird immerhin stets mitbedacht. So etwa auch im **Koalitionsvertrag für die 20. Wahlperiode des Schleswig-Holsteinischen Landtages** zwischen der CDU Landesverband Schleswig-Holstein und Bündnis 90/Die Grünen Landesverband Schleswig-Holstein:

„Dem Datenschutz kommt eine bedeutende Rolle im Digitalen zu. Das Recht auf informationelle Selbstbestimmung ist heute wichtiger denn je. Ein effektiver und moderner Datenschutz schützt die Menschenwürde und nimmt auch überindividuelle Risiken in den Blick. Der Schutz von Daten ist auch die Basis für Vertrauen bei digitalen Lösungen. Neben klaren rechtlichen Vorgaben bedarf es der Durchsetzung durch gut ausgestattete, unabhängige Aufsichtsstrukturen, denen auch eine wichtige Beratungsfunktion zukommt.“

Diesen Ausführungen kann uneingeschränkt zugestimmt werden.

### 3. Entwicklungen auf Europäischer und internationaler Ebene

#### a) Vom EU-US-Privacy Shield zum TADPF

Aufgrund einer Entscheidung des EuGH vom 16. Juli 2020, die das „EU-US-Privacy Shield“ für ungültig erklärte, **fehlt es bislang an einer Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA**. Das Privacy Shield, formal ein Angemessenheitsbeschluss im Sinne von Art. 45 DSGVO, fingierte ein gleichwertiges Schutzniveau für personenbezogene Daten in der EU und den USA. Der EuGH hatte das Abkommen jedoch mit sofortiger Wirkung aufgehoben, weil der Schutz in den USA wesentlich geringer sei. Erfordernisse der nationalen Sicherheit der USA, des dortigen öffentlichen Interesses und weitere Regelungen seien mit europäischen Rechtsprinzipien nicht vereinbar.

Seither wurde an einem Nachfolgeabkommen gearbeitet. Zu Beginn des Jahres 2022 wurde bekannt gegeben, dass ein „Trans-Atlantic Data Privacy Framework“ (TADPF) in Grundzügen erarbeitet sei. Am 25. März 2022 verkündeten die Europäische Kommission und der US-amerikanische Präsident, dass man sich im Grunde auf einen neuen EU-US-Datentransfer und -schutzrahmen geeinigt habe. Eckpunkte hierzu seien übereinstimmend ausgearbeitet worden. Im Oktober unterzeichnete der US-amerikanische Präsident eine Executive Order für das neue Abkommen. **Im ersten Quartal des Jahres 2023 könnte damit ein neuer Angemessenheitsbeschluss bestehen, der Datenübertragungen zwischen der EU und den USA legitimiert.**

Ob und wie lange das neue Abkommen Bestand haben wird, bleibt jedoch abzuwarten. Bereits vor dem Inkrafttreten gibt es vehemente Kritik an dem Entwurf, da mögliche staatliche Zugriffe nicht hinreichend beschränkt seien und effektiver Rechtsschutz nicht gewährleistet werde.

## b) Weitere EU-Gesetzgebungen

Auf europäischer Ebene gibt es weiterhin zahlreiche Gesetzgebungsvorhaben:

- **Digital Services Act:** Ziel ist ein besserer Verbraucherschutz im Internet durch die Haftung von Online-Plattformen für unrechtmäßige Inhalte (Angebot und Veräußerung gefälschter Produkte, Hass und Hetze) und mehr Transparenz beim Einsatz von Algorithmen und Online-Werbung.
- **Digital Markets Act:** Gatekeeper (Unternehmen mit einer dauerhaft wirtschaftlichen Bedeutung und erheblichen Auswirkungen auf den EU-Binnenmarkt) treffen mehr Verpflichtungen. Sie dürfen z. B. andere Anbieter nicht benachteiligen, Verbraucher\*innen nicht daran hindern, sich an Unternehmen außerhalb ihrer Plattformen zu wenden und vorab installierte Software oder Apps zu deinstallieren, wenn sie dies wünschen.
- **Artificial Intelligence Act:** Die Regulierung von künstlicher Intelligenz (KI) nach potenziellen Risiken zur Schaffung innovationsfreundlicher Umstände ist hier das Ziel.
- **Data Governance Act:** Hier geht es um die Regulierung der Verfügbarkeit von Daten zur wirtschaftlichen Nutzung, gemeinsamen Verwendung und für Forschungszwecke mit dem Ziel, dem europäischen Markt Wettbewerbsvorteile bei datengestützten Innovationen zu sichern.
- **Data Act:** Diese Maßnahme will den Datenfluss in der EU grundsätzlich erleichtern, indem gesetzliche, wirtschaftliche und technische Hemmnisse für die „Data Economy“ möglichst gering gehalten werden.

## 4. Bußgelder

Die Verhängung von Bußgeldern wegen der Verletzung datenschutzrechtlicher Vorgaben ist fast alltäglich geworden. Hier nur ein prominenten Beispiel:

Die irische Datenschutzbehörde hat Ende November 2022 ein Bußgeld in Höhe von **265 Mio. Euro gegen die Meta Platforms Ireland Ltd.** (Irland) wegen der Veröffentlichung von Nutzendendaten verhängt. Es war zu einer Veröffentlichung von personenbezogenen Daten (Namen, Telefonnummern, E-Mail-Adressen) von rund 533 Mio. Menschen gekommen. Die Daten wurden von Hackern abgegriffen aus Facebook Search, Facebook Messenger Contact Importer und Instagram Contact Importer. Die irische Datenschutzaufsichtsbehörde sah einen Verstoß gegen datenschutzrechtliche Anforderungen, weil keine hinreichenden technischen Sicherungsmaßnahmen ergriffen worden seien. Meta Platforms Ireland hat angekündigt, die Entscheidung überprüfen zu wollen.

Die Verhängung von Bußgeldern gegen Unternehmen gemäß Art. 58 Abs. 2 lit. i) in Verbindung mit Art. 83 DSGVO ist ein Aufsichtsmittel, um die einheitliche Überwachung und Durchsetzung der DSGVO sicherzustellen.

## **II. Rechtsprechung**

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

### **1. Zensus 2022**

Wie oben erwähnt, hatte sich das Bundesverfassungsgericht (BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983) vor fast 40 Jahren mit einer Volkszählung bzw. mit dem Volkszählungsgesetz 1983 befasst. Anfang des Jahres 2019 lehnte das Gericht einen Eilantrag gegen die teilweise Datenübermittlung für den Zensus 2021 ab:

„Die Bundesrepublik Deutschland ist verpflichtet, der Europäischen Kommission für das Bezugsjahr 2021 statistische Daten für eine geplante Volkszählung zu übermitteln. Zum Zweck der Prüfung der Übermittlungswege und der Qualität der hierfür zu übermittelnden Daten aus den Melderegistern sowie zum Test und zur Weiterentwicklung der Programme für die Durchführung des Zensus 2021 sieht § 9a des Zensusvorbereitungsgesetzes 2021 - beginnend am 14. Januar 2019 - eine zentrale Erfassung, Speicherung und Verarbeitung der nicht anonymisierten Meldedaten aller zum

13. Januar 2019 gemeldeter Personen durch das Statistische Bundesamt vor. Die übermittelten Daten sind nicht anonymisiert und umfassen neben Name und Wohnanschrift, Geschlecht, Staatsangehörigkeit und Familienstand u.a. auch die Zugehörigkeit zu öffentlich-rechtlichen Religionsgesellschaften. Eine Speicherung ist für einen Zeitraum von bis zu zwei Jahren nach dem Stichtag vorgesehen; eine Verarbeitung der Daten zu anderen Zwecken als der Prüfung der Übermittlungswege, der Prüfung der Datenqualität und dem Test und der Weiterentwicklung der Programme für die Durchführung des Zensus 2021 ist ausgeschlossen.

Die Antragsteller machen eine Verletzung ihres Rechts auf informationelle Selbstbestimmung geltend. Die Übermittlung der nicht anonymisierten Daten lasse Rückschlüsse auf den Kernbereich der privaten Lebensführung zu. Dies stehe außer Verhältnis zum Nutzen einer Erprobung und Optimierung der bereits weitgehend erprobten Übermittlungswege und Programme, zumal der Zweck der Übermittlung auch durch eine Übermittlung anonymisierter Daten - gegebenenfalls ergänzt um nicht anonymisierte Stichproben in geringem Umfang - in vergleichbarer Weise erreicht werden könne“

(<https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2019/bvg19-011.html>).

Das Gericht hatte das Für und Wider einer einstweiligen Anordnung abgewogen und war zu diesem Entschluss gekommen:

„Je weiter die Befugnisse staatlicher Stellen insoweit reichen, desto eher müssen die Bürgerinnen und Bürger befürchten, dass diese Stellen ihr Kommunikationsverhalten überwachen oder - wie im Fall der Erhebung für statistische Zwecke relevanter Daten - diese für Zwecke des Verwaltungsvollzugs auswerten oder mit Daten aus anderen Quellen verknüpfen. Mit der Speicherung allein ist in der Regel jedoch noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte“ (BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 06. Februar 2019).

Im Berichtsjahr befasste sich sodann das Verwaltungsgericht Neustadt (Weinstraße) (Beschluss vom 27.10.2022, Aktenzeichen: 3 L 763/22.NW) mit dem Zensus 2022 und kam zu diesem Ergebnis:

„Die Ausgestaltung des Zensus 2022 entspricht den Vorgaben, die das Bundesverfassungsgericht in seinem Urteil vom 19.9.2018 (a.a.O.) zum Zensus 2011 sowie in dem zur Volkszählung ergangenen Urteil vom 15.12.1983 (Az.: 1 BvR 209/83 u.a.) gemacht hat. Der Zensus 2022 ist wie der Zensus 2011 ein registergestützter Zensus (vgl. § 1 Satz 1 ZensVorbG 2022). Das BVerfG (Urteil vom 19.9.2018, a.a.O.) hat in dem zitierten Urteil das ZensG 2011 (wenngleich zuvörderst mit Blick auf die damalige Haushaltsstichprobe) letztlich nicht beanstandet. Die rechtlichen Schutzmechanismen des ZensG 2022 - bei vergleichbarer Eingriffsintensität des aktuellen Zensus - bleiben nicht hinter diejenigen des ZensG 2011 zurück. Das Bundesverfassungsgericht hat in seinen Grundsatzentscheidungen festgestellt, dass der Staat, um seinen Aufgaben nachkommen zu können, Informationen über die Bürger benötigt, die er im Wege einer Befragung erheben kann. Ferner hat das Bundesverfassungsgericht Anforderungen zur Verfahrensgestaltung aufgestellt, insbesondere dazu, in welcher Weise sicherzustellen ist, dass die Daten des Einzelnen (möglichst frühzeitig) anonymisiert werden, um dadurch den Schutz der Privatsphäre der Befragten zu sichern. Zudem ist erforderlich, dass die Erhebung auf der Grundlage eines förmlichen Gesetzes erfolgt, das den Verwendungszweck der betroffenen Informationen hinreichend präzise umgrenzt.“

## **2. Bundesverfassungsgericht zum Meldedatenabgleich**

Zur Erfüllung seiner Aufgaben benötigt nicht nur der Staat entsprechende Informationen über Bürger\*innen, sondern auch der staatsfern organisierte öffentlich-rechtliche Rundfunk. In § 11 Abs. 5 Rundfunkbeitragsstaatsvertrag (RBStV) ist daher ein Meldedatenabgleich geregelt. Dort heißt es:

„Zur Sicherstellung der Aktualität des Datenbestandes übermittelt jede Meldebehörde alle vier Jahre beginnend ab dem Jahr 2022 für einen bundesweit einheitlichen Stichtag automatisiert gegen Kostenerstattung in standardisierter Form die nachfolgenden Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt:

1. Familienname,
2. Vornamen unter Bezeichnung des Rufnamens,
3. frühere Namen,
4. Doktorgrad,

5. Familienstand,
6. Tag der Geburt,
7. gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung, und
8. Tag des Einzugs in die Wohnung.

Der Datenabgleich soll alle vier Jahre erfolgen. Dagegen ist Verfassungsbeschwerde erhoben worden. Das Bundesverfassungsgericht hat jedoch die Beschwerde aus formalen Gründen nicht zur Entscheidung angenommen, so dass die Norm weiterhin anzuwenden ist. Allerdings hat das Gericht Kritik geäußert:

„So soll der automatisierte Meldedatenabgleich dann nicht erfolgen, wenn der Datenbestand nach Prüfung durch die KEF „hinreichend aktuell“ ist (§ 11 Abs. 5 Satz 5 RBStV n.F.). Diese Prüfung findet alle zwei Jahre durch Berichterstattung an die Rundfunkanstalten statt (§ 11 Abs. 5 Satz 5 RBStV n.F. i.V.m. § 3 Abs. 8 des Rundfunkfinanzierungsstaatsvertrags - RFinStV). Dabei berücksichtigt die KEF die „Entwicklung des Beitragsaufkommens und sonstige Faktoren“ (§ 11 Abs. 5 Satz 6 RBStV n.F.). Was darunter genau zu verstehen ist, erschließt sich weder unmittelbar aus dem Norminhalt noch aus der Gesetzesbegründung. [...] Dabei wäre einerseits zu klären, ob und inwiefern die KEF die Möglichkeiten der Datenaktualisierung durch die soeben beschriebenen Anzeigepflichten und weiteren Erhebungsmethoden zu berücksichtigen in der Lage ist. Andererseits wäre zu prüfen, inwiefern der Meldedatenabgleich vor dem Hintergrund der zwischengeschalteten Prüfung durch die KEF der Sache nach automatisiert erfolgt und weiter ob und inwiefern eine sich an die „Fachentscheidung“ der KEF (s. die Begründung zum 23. RÄndStV, LTDrucks BW 16/7779, S. 17) als einem gemäß § 4 Abs. 1 RFinStV unabhängigen Sachverständigengremium anschließende Handlung der zuständigen Landesrundfunkanstalten gegenüber den Meldebehörden einen besonderen, selbständig gerichtlich angreifbaren Vollziehungsakt darstellt“ (BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 21. Januar 2022, Rn. 17).

Die **Kritik des Gerichts** lautet mithin, dass nicht zu erkennen sei, ob und inwieweit die KEF in der Lage ist, die erforderlichen Daten zu ermitteln.

### **3. Möglichkeiten des Datentransfers in die USA ohne Abkommen?**

Weil, wie oben berichtet, ein Nachfolgeabkommen zum aufgehobenen Privacy Shield noch nicht existiert, hatte die die Vergabekammer Baden-Württemberg (Beschluss vom 13. Juli 2022, Az. 1 VK 23/22) entschieden, dass ein US-Anbieter digitaler Server- und Clouddienstleistungen auch über europäische Tochtergesellschaften nicht datenschutzkonform erbringen könne. Nach Ansicht der Kammer handele es sich auch dann um eine unzulässige Übermittlung von personenbezogenen Daten in ein Drittland (außerhalb der EU), wenn der entsprechende Server von einer in der EU ansässigen Gesellschaft betrieben wird, die ihrerseits Teil eines US-Konzerns ist.

Wäre diese Entscheidung in Rechtskraft gewachsen, hätte eine Vielzahl von Systemen nicht betrieben werden können. Das OLG Karlsruhe beurteilte diese Sache allerdings anders (Oberlandesgericht Karlsruhe, Beschluss vom 7.9.2022, Aktenzeichen: 15 Verg 8/22): Das Gericht hob die Entscheidung auf, weil grundsätzlich davon auszugehen sei, dass ein Bieter seine vertraglichen Zusagen erfüllt. „Erst wenn sich aufgrund konkreter Anhaltspunkte Zweifel daran ergeben, muss der öffentliche Auftraggeber ergänzende Informationen einholen und die Erfüllbarkeit des Leistungsversprechens prüfen. Im jetzt entschiedenen Fall hatte die Anbieterin jedoch eindeutige Zusicherungen zu dem Inhalt des Vertrags zwischen ihr und der luxemburgischen Holding-Dienstleisterin gemacht. Danach dürfen Daten ausschließlich an diese luxemburgische Gesellschaft übermittelt und ausnahmslos von ihr und nur in Deutschland verarbeitet werden.“

Bis zum Inkrafttreten des Trans-Atlantic Data Privacy Framework ändert sich damit nichts.

### **4. Immaterieller Schadensersatz?**

Noch nicht geklärt ist die Frage, unter welchen Voraussetzungen Schadensersatz für Datenschutzverstöße zu leisten ist.

Diverse Verfahren sind diesbezüglich bei Gerichten anhängig. Erwartet wird vom Europäischen Gerichtshof (EuGH), dass Fragen zu den Voraussetzungen des datenschutzrechtlichen Schadensersatzanspruchs nach Art. 82 DSGVO geklärt werden.

Denn noch besteht keine Sicherheit, ob bereits jeder Verstoß gegen die DSGVO ausreicht, um einen Schadensersatzanspruch auszulösen. Ggf. wären auch Kriterien zu ermitteln, die eine **Erheblichkeitsschwelle** konkretisieren. Wann der EuGH entscheiden wird, ist derzeit nicht absehbar. Immerhin hat der Generalanwalt beim EuGH einen Vorschlag unterbreitet, wie Art. 82 DSGVO ausgelegt werden könnte:

„1. Für die Anerkennung eines Anspruchs auf Ersatz des Schadens, den eine Person infolge eines Verstoßes gegen die DSGVO erlitten hat, reicht die bloße Verletzung der Norm als solche nicht aus, wenn mit ihr keine entsprechenden materiellen oder immateriellen Schäden einhergehen.

2. Der in der DSGVO geregelte Ersatz immaterieller Schäden erstreckt sich nicht auf bloßen Ärger, zu dem die Verletzung ihrer Vorschriften bei der betroffenen Person geführt haben mag. Es ist Sache der nationalen Gerichte, herauszuarbeiten, wann das subjektive Unmutsgefühl auf Grund seiner Merkmale im Einzelfall als immaterieller Schaden angesehen werden kann.“

Aufgrund unterschiedlicher Entscheidungen bedarf es mithin der Klärung, ob schon ein Bagatellverstoß für den Zuspruch eines Schadensersatzanspruchs ausreichend ist oder der Verstoß „erheblicher“ bzw. spürbarer sein muss. Ob sich das Gericht dem Vorschlag anschließen wird, steht noch aus.

## **E. Tätigkeiten des Rundfunkdatenschutzbeauftragten des NDR im Jahr 2022**

Es wird zunächst auf die Zusammenarbeit mit anderen Datenschutzbeauftragten eingegangen.

### **I. Organisationsstrukturen/Zusammenarbeit mit anderen Aufsichtsbehörden**

Eine Zusammenarbeit bzw. ein Austausch erfolgt – wie bislang auch – in folgenden Kreisen:

- 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 Deutschlandradio (AKDSB)**: Das Forum aller Datenschutzbeauftragten von ARD,

ZDF, Deutschlandradio, dem ORF, ARTE und seit rund einem Jahr auch der Schweizerischen Radio- und Fernsehgesellschaft.

- Die **Datenschutzkonferenz (DSK)**: Das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder.

## 1. Die Rundfunkdatenschutzkonferenz (RDSK)

Die RDSK wird zukünftig weniger Mitglieder haben. Ende des Jahres 2022 wurde ein neuer Rundfunkdatenschutzbeauftragter des Bayerischen Rundfunks, des Saarländischen Rundfunks, des Westdeutschen Rundfunks, des Deutschlandradios und des Zweiten Deutschen Fernsehens ernannt. Dieser wird zugleich Aufsichtsbehörde über den SWR und MDR sein. Ob noch weitere Anstalten hinzukommen, ist unklar. Die weitere Zentralisierung wird diesseits als nachteilig empfunden, weil der Umfang der Tätigkeiten zunimmt, die Anzahl der damit befassten Personen hingegen geringer. Angesichts der Arbeitsverdichtungen ist die anstehende personelle Verkleinerung unbefriedigend. **Während zu Recht andere Aufsichtsbehörden wiederholt auf ihren erhöhten Personalbedarf hingewiesen haben, werden die entsprechenden Aufsichtsbehörden für den öffentlichen rechtlichen Rundfunk zusammengelegt und verkleinert.** Auch soweit dies vereinzelt als ein Teil einer „Strukturreform“ angesehen wird, erschließen sich weder die Vorteile noch der Reformgedanke: Denn die Entwicklung geht derzeit hin zu einem Weniger an Aufsicht. Dies ist angesichts der Bedeutung und des Zuwachses an Arbeit kein Vorteil. Auch der damit einhergehende Wunsch nach Auflösung der RDSK ist kein Gewinn. 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. Auch der Reformgedanke trägt nicht. **Die zuständigen Rundfunk- und Verwaltungsräte haben aus Gründen der Unabhängigkeit und Staatsferne über die Ernennung der Rundfunkdatenschutzaufsichten autonom zu entscheiden.** Diese Entscheidung einzuziehen, bedeutet einen Verlust an Autonomie und Kontrolle der Gremien.

Sollte überhaupt ein Bedarf an Änderungen der Datenschutzaufsicht über den öffentlich-rechtlichen Rundfunk erkannt werden, so lohnt der Blick auf bereits bestehende Modelle: Beim NDR, SWR und SR existieren bereits Regelungen, die hinsicht-

lich der Datenschutzaufsicht das Gebot der Staatsferne wirksam umgesetzt haben (es gibt keine geteilten Aufsichten) und zugleich bezüglich der personellen und finanziellen Ausstattung Möglichkeiten geben, ressourcenschonend zu arbeiten. Insgesamt gilt: **Wer Compliance ernst nehmen muss und ernst nimmt** – s. o. die Ausführungen in der Einleitung –, **der sollte einen gewichten Baustein aus dem Compliance-Risikokatalog nicht zusammenschmelzen.**

#### a) Organisation der RDSK

Weiterhin gelten die „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten“ und die „Verwaltungsvereinbarung zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten“. Aufgrund der geringeren Mitgliederzahl werden die Dokumente angepasst und die Arbeit verteilt werden müssen. Fraglich ist noch, wie das vereinbarte Prinzip der Federführung künftig gelebt werden kann.

#### b) Tätigkeitsschwerpunkte der RDSK

Aufgabe der RDSK ist u. a. auch **Öffentlichkeitsarbeit**, die insbesondere durch Empfehlungen, Stellungnahmen und Orientierungshilfen geleistet wird. Bereits jetzt wird diese Arbeit durch knappe Personalkapazitäten begrenzt.

Von besonderer Bedeutung war die Neufassung der **Empfehlungen zum Einsatz von Cookies und Local Storage-Elementen** in Online-Angebote der Rundfunkanstalten. Hintergrund ist das „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG). § 25 Abs. 1 TTDSG macht die Speicherung von Informationen in der Endeinrichtung von Nutzenden oder den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind (Cookies und Local Storage-Elemente), grundsätzlich von der ausdrücklichen Einwilligung der jeweils nutzenden Person abhängig. Ausnahmen dazu sieht das Gesetz ebenfalls vor, wenn die Speicherung oder der Zugriff auf die entsprechenden Informationen erforderlich ist. Bedeutend sind diese Regelungen, weil dies die **Etablierung von soge-**

**nannten Cookie-Bannern** hätte bedeuten können, etwa bei der Nutzungsmessung. Auf die Konsequenzen wird unter E. II. 2. C) eingegangen.

Alle Veröffentlichungen der RDSK sind zu finden unter **[www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen](http://www.rundfunkdatenschutzkonferenz.de/veroeffentlichungen)**.

Außerdem hat sich die RDSK beschäftigt mit diesen Themen:

- Zusammenarbeit mit der DSK und den Arbeitskreisen (s. u.)
- Nutzung von Drittplattformen durch die Rundfunkanstalten und Konsequenzen aus dem Urteil des OVG Schleswig-Holstein vom 25.11.2021 zu Facebook Fanpages
- Trans-Atlantic Data Privacy Framework (s. o.)
- Leitfaden für die datenschutzgerechte Gestaltung von Websites und Apps für Kinder des Rundfunkdatenschutzbeauftragten von BR, SR, WDR, DRadio und ZDF
- Initiative zum Erlass eines Verhaltenskodex nach § 12 Abs. 1 S. 7 MStV

### **c) Zusammenarbeit mit der Datenschutzkonferenz**

Zweimal im Jahr gibt es einen **Austausch mit der Datenschutzkonferenz** (DSK), dem Gremium der Datenschutzaufsichtsbehörden des Bundes und der Länder. Bei diesen Gelegenheiten werden mit den Aufsichtsbehörden der Länder, des Bundes, der Kirchen und des Rundfunks aktuelle Themen erörtert.

Auf der Tagesordnung standen aktuelle Entwicklungen im (europäischen) Datenschutz, Berichte über die Tätigkeitsschwerpunkte der Aufsichtsbehörden, etwa die Task Force Facebook Fanpages und das Vorhaben der DSK, von Landes- bzw. Bundesbehörden das Abschalten von Facebook Fanpages zu verlangen, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht sicherstellen können, und die Art und Weise der Zusammenarbeit.

Einige Mitglieder der RDSK nehmen an ausgewählten Sitzungen von Arbeitskreisen der DSK teil (AK Technik, AK Grundsatzfragen, AK Medien). Wie sich diesbezüglich der Austausch zukünftig gestalten wird, wird insbesondere auch

an der personellen Ausstattung der RDSK hängen. Jedenfalls wurde mit der DSK in Aussicht genommen, bei den Zusammentreffen weniger in die Vergangenheit zu schauen und mehr gemeinsam Themen zu bearbeiten. Dazu soll eine noch stärkere Einbindung in die Arbeit der Arbeitskreise erfolgen und die Vernetzung insgesamt intensiviert werden.

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

In den regelmäßig durchgeführten Sitzungen bzw. Videokonferenzen des AKDSB wurden im Schwerpunkt diese Themen erörtert:

- Aktuelle Entwicklungen der Rechtslage, Rechtsprechung und Politik
- Schadensersatzforderungen wegen der Verwendung von Google Fonts
- Datenschutzrechtliche Unterlassungsansprüche
- Tragweite des Auskunftsanspruchs
- Entscheidung des Bundesverfassungsgerichts zum Meldedatenabgleich
- Medienprivileg in Österreich
- Datenschutz und Rundfunkbeitragseinzug
- Klärung von Fragen grundsätzlicher Bedeutung / Orientierungshilfen
- Leitlinien zum Datenschutz in den Telemedien-Angeboten
- Orientierungshilfe zu Facebook Fanpages
- Orientierungshilfe zu Gewinnspielen
- Datenschutzkonformer Einsatz von Microsoft 365 / Datenschutzfolgenabschätzung
- Gemeinsames Login und Datenaustausch der Mediatheken von ARD und ZDF
- Datenschutzkonforme Vergabe / Beschaffung und Auftragskontrolle
- Einbeziehung von Datenschutz und Informationssicherheit in Projekte und Vorhaben
- Datenschutz bei der Baden-Badener Pensionskasse VVaG (der Pensionskasse der öffentlich-rechtlichen Rundfunkanstalten und Beteiligungsgesellschaften)
- Austausch zur Umsetzung der DSGVO
- ARD Diversity-Umfrage für Mitarbeitende

- Umsetzung von Whistleblower-Richtlinie und Hinweisgeberschutzgesetz
- SAP Harmonisierung
- Freelancer und Datenschutz
- Dreharbeiten in Schulen
- Desksharing

In den genannten **Leitlinien zum Datenschutz in den Telemedien-Angeboten** werden Handlungsempfehlungen für die technische und inhaltliche Gestaltung von Telemedienangeboten gemacht. Das ca. 70 Seite umfassende Papier geht auf alle relevanten Themen ein, die bei der Erstellung und Verbreitung von Telemedienangeboten zu beachten sind. Dabei handelt es sich etwa um Chats, Foren, Gästebücher, Kommentarfunktionen, spezifische Kontaktmöglichkeiten, den Einsatz von Cookies und anderen Technologien, Datenschutzerklärungen, Drittplattformen, Gewinnspiele, Anforderungen des Minderjährigen-Datenschutzes und Personalisierungen.

Außerdem wurde eine **Orientierungshilfe zu Facebook Fanpages** erarbeitet. Das Papier beleuchtet die rundfunkrechtlichen, datenschutzrechtlichen und verfassungsrechtlichen Aspekte bei der Nutzung von Facebook Fanpages durch die Rundfunkanstalten. Eine grundsätzliche Befassung mit dem Thema war notwendig, da der EuGH am 5. Juni 2018 geurteilt hatte, dass der Betreiber einer sogenannten Facebook-Fanpage gemeinsam mit Facebook datenschutzrechtlich verantwortlich ist. Es folgten weitere Urteile des BVerwG vom 11. September 2019 und des OVG Schleswig vom 25. November 2021. Rechtskräftiges Ergebnis ist, dass der Betrieb einer Facebook-Fanpage mit datenschutzrechtlichen Vorgaben grundsätzlich nicht zu vereinbaren ist. **Die Landesdatenschutzbehörden und der Bundesdatenschutzbeauftragte hatten daraufhin angekündigt, auf der Grundlage dieser Rechtsprechung gegen Facebook Fanpages von öffentlichen Einrichtungen vorzugehen.** In einer entsprechenden Veröffentlichung der Datenschutzkonferenz der Länder und des Bundes (DSK) aus dem März 2022 heißt es:

„Aufgrund ihrer Vorbildfunktion stehen öffentliche Stellen zuvörderst im Fokus. Deshalb werden die Mitglieder der DSK im Rahmen ihrer Zuständigkeit [...]

- überprüfen, ob Landes- bzw. Bundesbehörden Facebook-Fanpages betreiben,

- darauf hinwirken, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können.

Dieser Nachweis betrifft vor allem

- den Abschluss einer Vereinbarung nach Art. 26 DSGVO über die gemeinsame Verantwortlichkeit mit Facebook,
- ausreichende Informationen über die gemeinsamen Datenverarbeitungen gegenüber den die Fanpages Nutzenden gemäß Art. 13 DSGVO,
- die Zulässigkeit zur Speicherung von Informationen in der Endeinrichtung des Endnutzers und der Zugriff auf diese Informationen gemäß § 25 TTDSG sowie
- die Zulässigkeit der Übertragung personenbezogener Daten in den Zugriffsbereich von Behörden in Drittstaaten.“

**Zu klären war daher die Frage, ob die Präsenzen des öffentlich-rechtlichen Rundfunks rechtlich anders als im Falle sonstiger Auftritte öffentlicher Stellen zu bewerten sind.** Dies deshalb, weil zu berücksichtigen ist, dass der öffentlich-rechtliche Rundfunk zur Erfüllung seines verfassungsrechtlichen Auftrags gehalten ist, Telemedien auch außerhalb seiner eigenen Angebote bereitzustellen. Die Ausgestaltung dieses Auftrags findet sich in § 30 Abs. 4 S. 2 Medienstaatsvertrag. Dort heißt es: „Soweit dies zur Erreichung der Zielgruppe aus journalistisch-redaktionellen Gründen geboten ist, können sie Telemedien auch außerhalb des dafür jeweils eingerichteten eigenen Portals anbieten.“

Ferner war zu berücksichtigen, dass die Verbreitung der redaktionellen Inhalte über soziale Netzwerke der Auftragserfüllung des Rundfunks dienen, weil dort eine Vielzahl von Nutzer\*innen erreicht wird. **Damit kollidieren zwei verfassungsrechtlich geschützte Rechtsgüter:** Das Recht auf informationelle Selbstbestimmung und die Rundfunkfreiheit. Diese müssen in einer Abwägung so zugeordnet werden, dass beide Güter sich entfalten können. Mit dem Ende der entsprechenden Präsenzen würde der Auftrag des öffentlich-rechtlichen Rundfunks beschnitten werden und der Beitrag zur gemeinsamen datenschutzrechtlichen Verantwortung auf Drittplattformen entfielen. Im Sinne des **verfassungsrechtlich gebotenen Prinzips der prakti-**

**schen Konkordanz** war das Ergebnis der Abwägung, dass von einer nicht gleichwertigen Verantwortlichkeit auszugehen ist. Dies auch deshalb, weil die dortigen Auftritte nicht der bloßen Unternehmensdarstellung dienen, sondern der **Erfüllung des Auftrags nach § 26 Medienstaatsvertrag**. Zwar haben einige Drittplattformen erklärt, die gesamte datenschutzrechtliche Verantwortung für die Datenverarbeitungen übernehmen zu wollen. Ungeklärt ist aber noch, ob diese Erklärungen wirksam sind. **Die Orientierungshilfe zeigt daher auf, was bei Facebook-Auftritten zu beachten ist, um beide Rechtsgüter in Einklang zu bringen.**

**Weiterhin hat der NDR am Ende des Berichtsjahres angekündigt, neue Plattformen zu beschreiten**, die (derzeit) mit datenschutzrechtlichen Anforderungen besser zu vereinbaren sind.

Außerdem haben sich die Datenschutzbeauftragten der Kooperationspartner des IVZ (Informations-Verarbeitungs-Zentrum von ARD und Deutschlandradio) im sogenannten Jahrestreffen über die aus datenschutzrechtlicher Sicht relevanten Themen ausgetauscht.

## **II. Tätigkeitsschwerpunkte bezüglich Datenverarbeitungen im NDR**

Die Aufgaben des Rundfunkdatenschutzbeauftragten des NDR sind in § 46 NDR Staatsvertrag geregelt. Dort heißt es:

„Der oder die Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften dieses Staatsvertrages, des Medienstaatsvertrages, der Verordnung (EU) 2016/679 und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des NDR und seiner Beteiligungsunternehmen im Sinne des § 42 Absatz 3 Satz 1 des Medienstaatsvertrages. Er oder sie hat die Aufgaben und Befugnisse entsprechend der Artikel 57 und 58 Absatz 1 bis Absatz 5 der Verordnung (EU) 2016/679.“

Die Aufgaben und Befugnisse sind mithin klar gesetzlich definiert. In der Praxis liegt der **Schwerpunkt der Tätigkeit in der Beratung**. Dies ist auch bei anderen Aufsichtsbehörden so:

„Eine Aufgabe der Datenschutzbehörde ist, **kompetente Beratung zu Datenschutzthemen** zu veröffentlichen. Sie informiert die Öffentlichkeit über die Rechte und Pflichten im Bereich des Datenschutzes und insbesondere der Datenschutzgrundverordnung.“

([https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority\\_de#:~:text=Referenzen-,Antwort,und%20insbesondere%20der%20Datenschutz%2DGrundverordnung](https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority_de#:~:text=Referenzen-,Antwort,und%20insbesondere%20der%20Datenschutz%2DGrundverordnung))

„Um den Datenschutz **von Anfang an** sicherzustellen, berät die Landesbeauftragte die Landesregierung, Landesbehörden, Gemeinden und Gemeindeverbände sowie Unternehmen, die ihren Sitz in Brandenburg haben, im Umgang mit personenbezogenen Daten“.

(<https://www.lida.brandenburg.de/lida/de/ueber-uns/aufgaben-der-landesbeauftragten/>)

Die Beratung von Anfang an in allen relevanten Angelegenheiten sind mithin das Kerngeschäft. Grob unterteilt bedeutet dies, die Beratung hinsichtlich und Aufsicht über

- Programme und Programmverbreitung,
- den Einzug der Rundfunkbeiträge,
- Anforderungen des Beschäftigtendatenschutzes
- Organisations- und Strukturprojekte.

Der Bedarf an Beratungen ist unverändert hoch und intensiv. **Insbesondere deshalb kann ganz überwiegend von repressiven Aufsichtsmaßnahmen abgesehen werden.** Die datenschutzrechtliche Kontrolle von Anfang an bewährt sich, da die Kontrolldichte sehr eng ist. Beratung im Sinne von Prävention bringt eine Reihe von Vorteilen gegenüber anderen Reaktionen auf etwaig eingetretene Fehlentwicklungen mit sich.

## 1. Zur Umsetzung der DSGVO

Der im Jahr 2021 erkannte Handlungsbedarf bezüglich des **Führens des Verfahrenszeichnisses nach Art. 30 DSGVO** und der unterbreitete Vorschlag zur Erfüllung dieser Pflicht konnte erfreulicher Weise umgesetzt werden. Ergebnis ist

ein elektronisches Verzeichnis mit allen Pflichtangaben aus der DSGVO, das einen zusammenfassenden Überblick über die Verarbeitungen gibt und **zugleich eine Datenbank als Arbeitsmittel ist, in dem Beschäftigte relevante und geeignete Anwendungen zur Bewältigung der Arbeit finden können.**

Im Übrigen sind die Anforderungen des Datenschutzes im Geschäftsbetrieb immer zu gewährleisten. Datenschutz ist für den Verantwortlichen (und damit die Aufsichtsbehörden) keine einmalige Tätigkeit, sondern ständiger Begleiter aller Tätigkeiten und Aufsichtsmaßnahmen und Beratungsleistungen.

## **2. Programm und Programmverbreitung**

Beschwerden und Anfragen zu den vom NDR verantworteten Telemedienangeboten standen diesbezüglich im Fokus.

### **a) Datenschutzerklärungen und Informationspflichten**

Die Dynamik der Telemedienangebote und die Änderungen von Funktionalitäten erfordern regelmäßige Anpassungen und Ergänzungen der Datenschutzerklärungen gemäß den Prinzipien der Vollständigkeit, Transparenz und Verständlichkeit. Dies entfaltet entsprechenden Beratungsbedarf (s. dazu im Folgenden unter c)).

### **b) Informationsangebote der (Rundfunk-) Datenschutzbeauftragten**

Während in den Datenschutzerklärungen der Verantwortliche über seine Datenverarbeitungen zu informieren hat, sind die Angebote der Aufsichtsbehörden auf gesonderten Seiten zu finden, etwa denen der Rundfunkdatenschutzkonferenz und denen des Virtuellen Datenschutzbüros (ein gemeinsames Angebot von Datenschutzinstitutionen unter der Verantwortung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein):

- <https://www.rundfunkdatenschutzkonferenz.de/>
- <https://www.datenschutz.de/>
- [https://www.bfdi.bund.de/DE/Home/home\\_node.html](https://www.bfdi.bund.de/DE/Home/home_node.html)

- <https://www.datenschutzkonferenz-online.de/>

**c) Anfragen zu den Angeboten und Datenschutzerklärungen des NDR**

Rund 30 Zuschriften, d. h. Anfragen und Beschwerden, sind im Berichtsjahr eingegangen. Im Schwerpunkt waren die vom NDR verantworteten Telemedizinangebote und die entsprechenden Datenschutzerklärungen betroffen. Es ging insbesondere um:

- Nachfragen zu einzelnen Datenschutzbestimmungen
- die Erfüllung der Transparenz- und Informationspflichten des NDR
- Nutzungsmessungen
- Einwilligungserfordernisse nach dem TTDSG
- die Verwendung von Cookies
- technische Funktionalitäten, Serverdienste
- Datenschutz auf Drittplattformen bzw. die generelle Nutzung von Drittplattformen für programmliche Zwecke
- redaktionelle Inhalte, in denen Personen identifizierbar zu sehen waren
- Datenschutzbestimmungen für Foren
- Personalisierungen
- Wissenschaftliche Anfragen
- Datenschutz und Programmbeschwerden

Mehrere Anfragen beschäftigten sich mit der Frage, warum die **Telemedizinangebote auch ohne datenschutzrechtliche Einwilligungen** genutzt werden können und warum insbesondere für die Nutzungsmessung derartige Erfordernisse nicht bestehen. Zur Beantwortung dieser Fragen muss ausgeholt werden:

Zunächst ist grundsätzlich nachvollziehbar, dass der Verantwortliche eines Telemedizinangebots die Reichweiten statisch erheben möchte. Im Hörfunk und Fernsehen ist das ebenfalls üblich. Der NDR hat nachvollziehbar dargelegt, dass die Erhebung von anonymen, statistischen Daten der Erfüllung des verfassungsrechtlichen Funktionsauftrags des öffentlich-rechtlichen Rundfunks dient. Nach der Rechtsprechung des Bundesverfassungsgerichts darf

(und muss) der öffentlich-rechtliche Rundfunk seine Angebote im gesellschaftlichen Interesse auf allen publizistisch relevanten Plattformen zugänglich machen. Ob, wo und wie er damit seinen Auftrag erfüllt, hängt von der Konfiguration der Angebote ab. **Die Rundfunkanstalten sind dazu auf Erkenntnisse zur Akzeptanz und Nutzung angewiesen.** Dies gilt allerdings ausschließlich für anonymisierte Auswertungen. Die Rundfunkanstalten haben daher im Rahmen ihres verfassungsrechtlichen Funktionsauftrags ein berechtigtes Interesse am Einsatz von Cookies (oder vergleichbaren Messmethoden), die diese Aufgabe für ihre Telemedienangebote übernehmen. Sie verfolgen damit kein (markt-)wirtschaftliches, sondern ein ausschließlich publizistisches Ziel.

Für ein Einschreiten als datenschutzrechtliche Aufsichtsbehörde gegen die Nutzungsmessungen **auf der Grundlage der DSGVO** gab es daher keine Anhaltspunkte: Für die Rundfunkanstalten ist die anonymisierte Nutzungsmessung erforderlich, damit sie die ihnen durch die Verfassung übertragene Aufgabe optimal wahrnehmen können. Auch nach Maßgabe einer Interessenabwägung ist die Nutzungsmessung zulässig. Nach einem einschlägigen Urteil des EuGH kann das allgemeine Interesse des Verantwortlichen an einer Erfassung und Auswertung des Nutzungsverhaltens zwar nicht per se als „berechtigtes Interesse“ im Sinne von Art. 6 Abs. 1 S. 1 lit. f) DSGVO qualifiziert werden. **Im Falle einer ausschließlich publizistisch motivierten anonymisierten Nutzungsmessung überwiegt jedoch das Interesse der Rundfunkanstalt (und der Gesamtheit ihres Publikums) ein etwa entgegenstehendes individuelles Interesse.**

Neben den Anforderungen der DSGVO war die **Einhaltung des TTDSG** zu prüfen. Unter E. I. 1. b) wurde bereits das „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG) erwähnt. Dieses Gesetz enthält u. a. weitere besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien und zum Schutz der Privatsphäre bei Endrichtungen.

Im TTDSG findet sich eine Regel: Sofern Informationen in der Endeinrichtung (gemeint sind z. B. Smartphones, Tablets, PC) von Nutzenden abgelegt oder Zugriffe auf Informationen, die bereits in der Endeinrichtung gespeichert sind (Cookies und Local Storage-Elemente), vorgenommen werden sollen, bedarf es grundsätzlich einer entsprechenden Einwilligung. Da der NDR allerdings keine sogenannten Cookie-Consent-Banner einsetzt, um Einwilligungen einzuholen, gab es entsprechende Anfragen und Beschwerden.

Zutreffend ist, dass der NDR für den Zweck der Nutzungsmessung auf Informationen ohne Personenbezug im Endgerät der Nutzenden zugreift. Dies ist nach Maßgabe des § 25 Abs. 2 TTDSG zulässig. Danach bedarf aber grundsätzlich eine solche Datenverarbeitung zum Schutz der Privatsphäre der Nutzenden einer Einwilligung, es sei denn, es liegt ein gesetzlich geregelter geregelter Ausnahmefälle vor.

Das Erfordernis der Einholung einer Einwilligung konnte aber nicht erkannt werden, weil die Datenverarbeitung **nur zu journalistischen Zwecken** durchgeführt wird. Überdies ist davon auszugehen, dass „Rundfunk- und Presseunternehmen sowie deren Datenverarbeitung zu journalistischen Zwecken von den Regelungen (des) TTDSG nicht erfasst werden, wie dies auch schon unter Geltung der Vorgängerregelungen im TKG und TMG der Fall war“ (Stellungnahme des Bundesrates vom 26.3.2021 (Nr. 11)). Grund dafür ist das **Medienprivileg**, welches das durch Art. 11 Abs. 2 GRCh auf europäischer und durch Art. 5 Abs. 1 S. 2 GG auf nationaler Ebene geschützte Interesse an einer freien und ungehinderten Medienberichterstattung (auch im Bereich der Telemedien) wahren soll.

**Auch nach Maßgabe des § 25 Abs. 2 TTDSG ist es dem Verantwortlichen daher möglich, die ausschließlich anonymisierte Nutzungsmessung zu publizistischen Zwecken durchzuführen, ohne eine Einwilligung einzuholen.** Denn die entsprechende Datenverarbeitung dient dem bereits erläuterten Zweck der Erfüllung des Funktionsauftrags des öffentlich-rechtlichen Rundfunks zur Positionierung im publizistischen Wettbewerb. Diese Datenverarbeitung ist auch „unbedingt erforderlich“ im Sinne des Gesetzes, um einen ausdrücklich gewünschten Telemediendienst zur Verfügung zu stellen. Nach der

Rechtsprechung des Bundesverfassungsgerichts ist der Rundfunk „Medium und Faktor der öffentlichen Meinungsbildung“. Wie die Angebote angenommen und rezipiert werden, muss daher ermittelt werden. Der Einfluss der für den publizistischen Erfolg und die Relevanz redaktioneller Angebote sind bedingt durch unterschiedliche Faktoren der Konfiguration, Gestaltung, Platzierung und Formulierung der einzelnen Inhalte eines Gesamtangebots, die je für sich erfasst und ausgewertet werden müssen. Wäre für diese notwendige Auswertung der Daten das Einholen von Einwilligungen erforderlich, bestünde das erhebliche Risiko des Wegfalls einer validen, aussagekräftigen Datenlage zur Nutzungsmessung. **Für die Nutzungsmessung gilt daher auch nach Maßgabe des TTDSG, dass diese ausschließlich im publizistischen Interesse vorgenommen wird und erforderlich im Sinne dieses Gesetzes ist.**

Auch die **Erhebung weiterer technischer Informationen, wie etwa Gerätehersteller und Provider, wird vorgenommen, um technische Fehler zu analysieren und die Stabilität des Angebots zu gewährleisten.** Da einige technische Probleme nur bei bestimmten Gerätetypen und/oder bestimmten Displaygrößen auftreten oder nur einem Provider zuzuordnen sind, werden die Daten zur Sicherheit und Fehlerbehebung verarbeitet. Auch nach Maßgabe des TTDSG besteht daher insoweit kein Erfordernis der Einholung von Einwilligungen, denn die Telemedienangebote sollen im Interesse der Nutzenden sicher, schnell und stabil zur Verfügung gestellt werden.

**Zusammenfassend gilt daher, dass die derzeit bestehenden Konfigurationen der Angebote keine Cookie-Banner erforderlich machen.**

Viele Anfragen betrafen insbesondere **Berichterstattungen, Dokumentationen, aber auch fiktionale Angebote** des NDR, in denen Personen kenntlich zu sehen waren. Die Beiträge bzw. einzelne in diesen benannte Passagen wurden geprüft. Hinsichtlich dieser Anfragen hat sich die Rechtslage nach Inkrafttreten der DSGVO nicht verändert. Diesbezüglich scheint es allerdings Fehlvorstellungen zu geben: Bildveröffentlichungen in Medien sind nach einem abgestuften Schutzkonzept zu beurteilen. **Dies gilt im Grundsatz seit dem Jahr 1907** (s. oben unter D. – Ablichtung des Reichskanzlers Otto von Bismarck in seinem Sterbezimmer). Bildnisse einer Person dürfen grundsätz-

lich nur mit deren Einwilligung verbreitet werden. Die Veröffentlichung des Bildes einer Person begründet regelmäßig eine rechtfertigungsbedürftige Beschränkung ihres allgemeinen Persönlichkeitsrechts. Die nicht von der Einwilligung des Abgebildeten gedeckte Verbreitung seines Bildes ist nur zulässig, wenn dieses Bild dem Bereich der Zeitgeschichte oder einem der weiteren Ausnahmetatbestände zuzuordnen ist und berechnete Interessen des Abgebildeten nicht verletzt werden (§ 23 KUG). Dabei ist schon bei der Beurteilung, ob ein Bild dem Bereich der Zeitgeschichte zuzuordnen ist, eine Abwägung zwischen den Rechten des Abgebildeten einerseits und den Rechten der Medien (Art. 5 GG) andererseits vorzunehmen.

Diese Vorgaben gelten seit rund 116 Jahren und auch nach Maßgabe der DSGVO. Stets muss also eine Abwägung vorgenommen werden zwischen dem Persönlichkeitsrecht von abgebildeten Personen und dem Berichterstattungsinteresse von Medien.

**Sprache ist ein sensibles und emotionales Thema.** Der NDR hat „Anregungen für einen geschlechtergerechten Sprachgebrauch“ herausgegeben ([https://www.ndr.de/der\\_ndr/unternehmen/organisation/geschlechtergerechtesprache100.pdf](https://www.ndr.de/der_ndr/unternehmen/organisation/geschlechtergerechtesprache100.pdf)). Auch die Datenschutzerklärungen orientieren sich daran. Art. 12 DSGVO gibt dem Verantwortlichen auf, „alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“. Dass diese Anforderungen nicht erfüllt werden, war nicht festzustellen: Nach aktueller Rechtslage gibt es wohl **kein Recht auf eine geschlechtergerechte Sprache** (so das BVerfG, Beschluss vom 26. Mai 2020 - 1 BvR 1074/18, abrufbar unter [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rk20200526\\_1bvr107418.html;jsessionid=9EC7AE8BC2DC24FC56EAF8C50651BD56.1\\_cid329](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rk20200526_1bvr107418.html;jsessionid=9EC7AE8BC2DC24FC56EAF8C50651BD56.1_cid329)). Es gibt jedoch auch **keinen Anspruch, diese zu unterlassen** (so das LG Ingolstadt, Endurteil v. 29.07.2022 - 83 O 1394/21, abrufbar unter <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2022-N-19421?hl=true>). **Der vom NDR für seine Datenschutzerklärungen benutzte geschlechtergerechte Sprachgebrauch entspricht daher auch den Maßgaben der DSGVO.**

#### d) Anfragen von Redaktionen

Im Erwägungsgrund Nr. 153 zur DSGVO heißt es: „... Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.“ Datenverarbeitungen zu journalistischen Zwecken genießen daher Privilegien. Es gelten z. B. die umfangreichen Informations- und Dokumentationspflichten, Auskunfts- und Widerrufsrechte für Betroffene nicht. Dies ist der Kern des sogenannten Medienprivileg (Art. 85 DSGVO). Dafür gelten andere Regelungen (etwa das Recht auf Gegendarstellung). **Starre Grenzen kennt das Medienprivileg kaum. Vielmehr sind im Einzelfall die Grenzen zu ermitteln.** Geschützt und privilegiert sind Medien jedenfalls im gesamten Prozess der redaktionellen Arbeit (Recherche, Redaktion, Veröffentlichung, Dokumentation und Archivierung), wenn sie mit ihren Tätigkeiten die Weitergabe von Informationen, Meinungen und Vorstellungen an die Öffentlichkeit bezwecken.

Die Grenzziehungen und die Einhaltung notwendiger Vorschriften sind Gegenstand der Beratungen. Hier ein Auszug:

- Neuerungen bei der ARD Quiz App / Mediathek
- Anforderungen an Kontaktschnittstellen mit dem Publikum
- Modalitäten für die Anmeldung für das Bürgerparlament
- Datenübermittlungen für Akkreditierungszwecke und zur Sicherheitsüberprüfung
- Datenschutzfragen zum ESC
- Anmeldungen und Registrierungen zu Web-Workshops und Contests
- Datenschutz bei Kartenverlosungen
- Sichere Erfassung von Gewinner\*innen-Daten
- Anforderungen an Community-Management-Systeme
- Datenschutzhinweise und weitere Anforderungen zu #NDRfragt (#NDRfragt ist eine neue Umfrage- und Dialogplattform des NDR. Nach einer Anmeldung regelmäßig Einladungen zu Umfragen versandt, die Ergebnisse ausgewertet und redaktionell genutzt)
- Gestaltung von Bewerbungsformularen (z. B. NDR Young Reporter)

- Datenschutzkonforme Regelungen für Auftragsproduktionen
- Hinweise und Erklärungen für Kandidat\*innen in Sendungen des NDR
- Anforderungen an ein Dialog-Projekt des NDR mit Videobotschaften

Die entsprechenden Beratungen wurden geleistet die Ergebnisse umgesetzt.

### **3. Rundfunkteilnehmerdatenschutz**

Neben der grundsätzlichen Behandlung der datenschutzrechtlichen Anforderungen beim Einzug der Rundfunkbeiträge sind Beschwerden zu bearbeiten.

Die Anzahl der Auskunftsanfragen den NDR betreffend ist recht stabil: An den Beitragsservice in Köln haben im Jahr 2021 insgesamt 6.888 Personen erfragt, welche personenbezogenen Daten über sie verarbeitet werden. Von diesen Auskunftersuchen entfielen 1.116 auf den NDR. Im Jahr 2022 waren es 939. Insgesamt hat sich die Anzahl der Auskunftersuchen beim Beitragsservice um rund 1000 Anfragen reduziert.

Im Jahr 2022 hatte der NDR in Hamburg 10 allgemeine Auskunftsanfragen zu beantworten und 14 weitere Ersuchen, die ausschließlich den Beitragseinzug durch den NDR betrafen. Dies entspricht etwa dem Niveau des Jahres 2021.

Gleiches gilt für die Beschwerden mit beitragsrechtlichem Bezug. 15 Beschwerden waren zu bearbeiten (im Jahr 2021 waren es 20 Eingaben). Schwerpunkt der Beschwerden war der Vorwurf, dass nicht umfassend beauskunftet worden sei. Dies konnte jedoch nicht bestätigt werden. Denn das Recht auf Erhalt einer Auskunft wurde nicht selten mit einem Recht auf Akteneinsicht verwechselt. Der Inhalt einer vom Verantwortlichen zu erteilenden Auskunft richtet sich beim Beitragseinzug nach § 11 Abs. 8 Rundfunkbeitragsstaatsvertrag. 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.“

Damit umfasst der Auskunftsanspruch – auch aus Art. 15 DSGVO – nicht das Recht, Kopien von einzelnen oder sämtlichen Schriftstücken zu erhalten. Das datenschutzrechtliche Auskunftsrecht ist **kein Recht auf Akteneinsicht und kein Recht auf Übersendung von Kopien aller zu einer Person verarbeiteten Schriftstücke**. Art. 15 Abs. 3 S. 1 DSGVO lautet: „Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.“ Damit ist nicht gemeint, dass ein Doppel eines oder mehrerer Schriftstücke erstellt und einer Betroffenen übersandt werden müsste. Der Begriff der Kopie des Art. 15 Abs. 3 S. 1 DSGVO meint **eine strukturierte Zusammenfassung** der personenbezogenen Daten, nicht aber eine Übersendung aller Dokumente in Kopie.

#### 4. Beschäftigtendatenschutz

Der Beschäftigtendatenschutz hat auch im Jahr 2022 eine große Rolle gespielt und wird dies voraussichtlich auch weiterhin tun. Im Schwerpunkt ging es um Regelwerke und Systeme, mit denen einzelne Bereiche oder die gesamte Belegschaft miteinander arbeiten.

##### a) Tarifvertrag hybride Arbeit

Unter Umständen können Beschäftigte des NDR ihre Tätigkeit auch außerhalb der Betriebsstätten des NDR verrichten. Die Voraussetzungen und Regelungen dazu finden sich im Tarifvertrag über hybride Arbeit ([https://www.ndr.de/der\\_ndr/unternehmen/hybridarbeit100.pdf](https://www.ndr.de/der_ndr/unternehmen/hybridarbeit100.pdf)). Die Regelungen des Tarifvertrages sehen vor, dass Beschäftigte, die hybrid (d. h.

auch mobil) arbeiten wollen, einen entsprechenden **Führerschein** absolvieren müssen. Zu beachten sind besondere Belange des Datenschutzes und der IT-Sicherheit sowie Regelungen zum Arbeits- und Gesundheitsschutz. Beratungen wurden geleistet zu den Inhalten des Führerscheins aus datenschutzrechtlicher Sicht und die entsprechenden Anforderungen skizziert. Ein Bestandteil des Führerscheins ist, dass jährlich wiederkehrend entsprechende Schulungen zu absolvieren sind. Dazu kann ein Online-Angebot genutzt werden. Darüber hinaus ist mit dem NDR die Verständigung erzielt worden, dass – unabhängig von hybrider Arbeit oder Telearbeit – **alle Beschäftigten derartige Schulungen durchführen müssen**.

Die Regelungen sind insgesamt zu begrüßen, weil damit Klarheit geschaffen wurde. Denn der im Jahr 2020 vom NDR erarbeitete Entwurf einer Dienstvereinbarung zum Homeoffice wurde nicht in Kraft gesetzt. Die nun geltenden Regelungen und Verfahren sind geeignet und erforderlich, um das in allen Arbeitssituationen notwendige Sicherheitsniveau zu gewährleisten.

#### **b) IT-Rahmendienstvereinbarung**

Die IT-Rahmendienstvereinbarung regelt Grundsätze bei der Einführung, Anwendung und Änderung von informationstechnischen Systemen (IT-Systemen). Die Regelungen waren zu überarbeiten und zu aktualisieren. Die Dienstvereinbarung wurde zwar noch nicht abgeschlossen. Es wurde aber angeraten, insbesondere Regelungen zur **Nutzung privater Endgeräte** für dienstliche Zwecke aufzunehmen und Grundsätze zu vereinbaren, nach denen personenbezogene Daten gespeichert werden dürfen, um **Systeme zur Erkennung von Cyberangriffen** einzusetzen.

In Bearbeitung sind weitere Dienstvereinbarungen. So soll aufgrund des „Projekts der Harmonisierung und Konsolidierung der Geschäftsprozesse und der dezentralen SAP-Systeme der einzelnen Rundfunkanstalten in eine zentrale SAP-Systemlandschaft“ eine entsprechende Dienstvereinbarung geschlossen werden. Gleiches gilt für den Einsatz von Microsoft 365-Anwendungen.

### c) Sichere elektronische Kommunikation von Personaldaten

In vielen Bereichen wird die Digitalisierung und damit auch die elektronische Kommunikation intensiviert. Ein solches Vorhaben verfolgt auch die Personalabteilung. Der Prozess hat im Berichtsjahr begonnen und wird im kommenden Jahr fortgesetzt. Aufgrund der teils **sensiblen und vertraulichen Daten**, die die Personalabteilung mit Beschäftigten kommuniziert, können nicht in allen Fällen die vorhandenen Kommunikationskanäle – jedenfalls nicht ohne besondere Schutzmaßnahmen – genutzt werden. Das – über 300 alte (s. o.) – Brief-, Post- und Fernmeldegeheimnis muss auch in der digitalen Kommunikation gewahrt werden. Welche Möglichkeiten bestehen und welche Maßnahmen zu ergreifen sind, wurde erörtert.

### d) Auskunftersuchen von beschäftigten Personen

Auch im NDR beschäftigte Personen haben sich an ihren Arbeitgeber gewandt, um eine Auskunft nach Art. 15 DSGVO zu den zu ihrer Person verarbeiteten Daten zu erhalten. In manchen Fällen wurde die Auskunft hinsichtlich einer konkreten Verarbeitungstätigkeit erfragt, was der NDR ohne großen Aufwand erledigen konnte. Nachfragen und entsprechenden Beratungsbedarf gab es jedoch sowohl auf Seiten der Auskunftssuchenden, als auch beim Verantwortlichen. Dies deshalb, weil **die Form der Erfüllung des Anspruchs** unklar war. Dies mag am Wortlaut des Art. 15 DSGVO liegen. Jedenfalls gilt:

Der Auskunftsanspruch umfasst nicht das Recht, Kopien von Schriftstücken zu erhalten, s. o. Das datenschutzrechtliche Auskunftsrecht ist kein Recht auf Akteneinsicht und kein Recht auf Übersendung von Kopien aller zu einer Person verarbeiteten Schriftstücke. Mit der Übersendung einer strukturierten Zusammenstellung ist daher der Anspruch auf Auskunft erfüllt. Denn die auskunftssuchende Person wird damit in die Lage versetzt, sich der Verarbeitung ihrer personenbezogenen Daten bewusst zu werden und die Rechtmäßigkeit der Datenverarbeitung zu überprüfen.

Art. 15 Abs. 3 DSGVO meint also eine **vollständige und übersichtlich geordnete Zusammenfassung** der verarbeiteten Daten. Daher müssen betroffenen

Personen nicht sämtliche, ihn betreffenden Dokumente in Kopie zur Verfügung gestellt werden.

#### e) **Löschung von Daten im Zusammenhang mit der Corona-Pandemie**

Im Laufe des Berichtsjahres entfielen eine Reihe von Regelungen, die der Gesetzgeber zwecks Eindämmung der Corona-Pandemie erlassen hatte. Aufgrund des Wegfalls der Regelungen entfielen auch die Rechtsgrundlagen für die Verarbeitung entsprechender Daten. Es war daher darauf hinzuwirken, dass die **personenbezogenen Daten, die im Zusammenhang mit Maßnahmen zur Pandemiebekämpfung verarbeitet wurden, gelöscht werden** (etwa solche zur Zutrittskontrolle am Arbeitsplatz („3G-Kontrolle)). Entsprechende Daten waren daher unverzüglich und qualifiziert zu löschen.

Erhalten blieben allerdings noch Fehlzeitenmeldungen aufgrund von Absonderungen. Ganz grundsätzlich gilt, dass personenbezogene Daten von Beschäftigten – dazu zählen auch Daten über die Gesundheit von Mitarbeiter\*innen – nur verarbeitet werden dürfen, wenn eine Einwilligung der betroffenen Personen vorliegt oder eine Rechtsgrundlage dies gestattet.

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

Der Arbeitgeber hat ein begründetes Interesse an der Feststellung, ob er einer beschäftigten Person, die sich in einem Risikogebiet aufgehalten hat oder Kontakt zu einer erkrankten Person hatte, Verdienstaufschlüsselung nach § 56 Abs. 5 S. 1 Infektionsschutzgesetz (IfSG) zahlen muss, weil sich die beschäftigte Person absondern hat. Die Kenntnis des Impfstatus ist damit

für den Entschädigungsanspruch der beschäftigten Person und für den Erstattungsanspruch des Arbeitgebers gegenüber den für eine Erstattung zuständigen Behörden maßgeblich (§ 56 Abs. 5 S. 2 und Abs. 12 IfSG). Denn eine Entschädigung ist nicht zu leisten, wenn keine Quarantänepflicht mehr besteht. Dies ist nach dem RKI dann der Fall, wenn eine Person vollständig geimpft ist.

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

Insgesamt ist daher festzuhalten, dass § 56 IfSG die Rechtsgrundlage enthält, entsprechende Datenverarbeitungen vorzunehmen. Datenschutzrechtliche Bedenken sind daher im vorliegenden Fall nicht erkennbar.

#### f) Schulungen

Schulungsveranstaltungen wurden für die neuen Auszubildenden und Volontär\*innen durchgeführt. Diese persönlichen Schulungsveranstaltungen sollen zur Stärkung der Achtsamkeit für neu im NDR beschäftigte Personen beibehalten werden, auch wenn im Übrigen Online-Schulungen regelmäßig von allen absolviert werden müssen. Die Online-Schulungen erfahren Ergänzungen derart, dass **Informations- und Beratungstermine gemeinsam mit dem IT-Sicherheitsbeauftragten** durchgeführt werden, in denen auf besondere Bedarfe und Einzelfragen aus einzelnen Bereichen des NDR eingegangen wird. Entsprechende Beratungstermine wurden bereits durchgeführt.

Damit sind weitere organisatorische Maßnahmen zur Erhöhung der Sensibilität für datenschutzrechtliche Anforderungen und Abwehr von Gefahren ergriffen worden. Dies ist wichtig. Denn der NDR muss als Verantwortlicher auch **organisatorisch** dafür sorgen, dass datenschutzrechtliche Vorgaben umgesetzt werden. Neben technischen Anforderungen und unternehmensinternen Regelungen sind dafür stetige Maßnahmen der Beschäftigten erforderlich. Ein Instrument ist dabei die seit dem Jahr 2018 praktizierte „Verpflichtung

auf die Vertraulichkeit“, die von allen Personen bei Aufnahme der Tätigkeit im NDR zur Kenntnis genommen und unterzeichnet werden muss. Die Durchführung der organisatorischen **Maßnahmen sind entsprechend zu dokumentieren**.

#### g) **Warnstreiks**

Im NDR kam es zu Warnstreiks. Diesbezüglich gab es Verwirrungen, weil aufgefordert worden war, „alle Streikenden im NDR in einer Übersicht zu erfassen“. Dies war nicht so gemeint und wurde auch nicht so vorgenommen. Auf Nachfrage wurde auch bestätigt, dass eine derartige Meldung von einzelnen Personen nicht passiert war.

§ 320 Abs. 5 SGB III lautet: „Arbeitgeber, in deren Betrieben ein Arbeitskampf stattfindet, haben bei dessen Ausbruch und Beendigung der Agentur für Arbeit unverzüglich Anzeige zu erstatten. Die Anzeige bei Ausbruch des Arbeitskampfes muss Name und Anschrift des Betriebes, Datum des Beginns der Arbeitseinstellung und Zahl der betroffenen Arbeitnehmerinnen und Arbeitnehmer enthalten. Die Anzeige bei Beendigung des Arbeitskampfes muss außer Name und Anschrift des Betriebes das Datum der Beendigung der Arbeitseinstellung, die Zahl der an den einzelnen Tagen betroffenen Arbeitnehmerinnen und Arbeitnehmer sowie die Zahl der durch Arbeitseinstellung ausgefallenen Arbeitstage enthalten.“

Diese Meldung an die Agentur für Arbeit erfolgt also anonym und wurde auch so getätigt. Allerdings erfasst der NDR intern Angaben der Streikenden und der ausgefallenen Arbeitstage bzw. -stunden. Dies passiert, um den **Gehaltsabzug** berechnen. Einen Verstoß gegen datenschutzrechtliche Vorgaben stellt dies nicht da. Die Streikteilnahme darf **nicht in die Personalakte** aufgenommen werden, sondern dient allein internen Abrechnungszwecken.

#### h) **Umfragen unter Beschäftigten**

Allgemeine Zufriedenheitsumfragen (z. B. in den Servicebereichen) ohne Bewertung konkreter Personen, d. h. ohne personenbezogene Daten auf Seiten

der Befragten und der Bewerteten, sind möglich, sofern der Kreis der Personen so groß ist, dass keine Rückschlüsse auf konkrete Personen gezogen werden können.

Für spezielle Umfragen, Abfragen, Abstimmungen etc. unter Beschäftigten wurden ebenfalls Hinweise gegeben. Die Anforderungen sind hier weitaus strenger. Der Verantwortliche muss Folgendes beachten:

- Zweck und Zweckbindung der Datenerhebung: Was soll mit der Umfrage erreicht werden?
- Begrenzung auf einen Kreis von Teilnehmenden, von denen vernünftiger Weise (etwa aufgrund einer Zusammenarbeit) von einer profunden Rückmeldung ausgegangen werden kann.
- Im Umkehrschluss: Wer darf nicht teilnehmen?
- Absicherung, dass nicht mehrfache Rückmeldungen von einer Person erfolgen.
- Zwecks Auswertung und Verhinderung von stigmatisierenden Rückmeldungen: bestenfalls vorgegebene Fragen mit Antwortmöglichkeiten zum Anklicken.
- Bei der Auswertung:
  - Zuständigkeiten (Berechtigungen) definieren beim Zugriff auf die erhobenen Daten und deren Auswertung.
  - Wer darf was von anderen (Führungskräften) wissen? Kriterien einer etwaigen Weitergabe („Diskussion der Ergebnisse“) festlegen.
- Wo werden die Daten gespeichert?
- Wo und wie werden die Daten (ggf. betriebsintern) veröffentlicht?
- Wann werden sie qualifiziert vernichtet?
- Bei den Befragten: Freiwilligkeit, Transparenz, Anonymität gewährleisten.

Festzustellen war, dass mit den bislang vorhandenen Tools anonyme Abfragen, Abstimmungen, Wahlen etc. nicht möglich sind. Dies deshalb, weil die Anonymität nicht gewahrt ist. Denn auch ohne Wissen der Beschäftigten können Namen in digitalen Systemen erfasster Personen gespeichert werden. Zudem werden weitere personenbezogene Daten (z. B. IP-Adressen) re-

gelmäßig erfasst und auch Cookies gesetzt. Damit besteht die Möglichkeit einer Rückverfolgbarkeit und folglich auch keine Anonymität.

#### i) **Elektronische Arbeitsunfähigkeitsbescheinigungen**

Zu Beginn des Jahres 2023 gibt es Änderungen hinsichtlich des Verfahrens zur Ausstellung von Arbeitsunfähigkeitsbescheinigungen. Derartige Bescheinigungen sollen überwiegend elektronisch übermittelt werden, und zwar von der ausstellenden Arztpraxis an die Krankenkassen. Beschäftigte Personen sollen lediglich ihren Arbeitgeber über die Arbeitsunfähigkeit informieren. Dieser ruft wiederum auf elektronischem Wege die Arbeitsunfähigkeitsbescheinigung bei der Krankenversicherung ab.

Zumindest theoretisch sind nach Prüfung der digitalen Kommunikationswege keine Probleme zu erwarten, auch wenn es sich um besonders schützenswerte Daten handelt. Es gelten diesbezüglich die „Gemeinsamen Grundsätze Technik für die elektronische Datenübermittlung gemäß § 95 SGB IV“, die hinreichende Vertraulichkeit und Sicherheit gewährleisten sollten.

### 5. **Weitere Beratungen und Prüfungen im NDR**

Zum Regelgeschäft gehören Beratungstätigkeiten, die insbesondere Digitalisierungs-, Organisations- und Strukturänderungsvorhaben betreffen. Hierbei wird fast die gesamte Tätigkeit des NDR datenschutzrechtlich gespiegelt, weil eine Vielzahl von Bereichen des NDR entsprechende Anfragen gestellt haben. Dies führt zu einem erheblichen Arbeitsaufwand, dessen Grundlage in Art. 25 DSGVO zu finden ist. Die Anforderungen an „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ muss der NDR berücksichtigen und umsetzen. Wie das passieren kann, ist Bestandteil der Beratungsleistung. Ziel ist, dass der Verantwortliche **interne Strategien festlegt und Maßnahmen ergreift, die insbesondere den Grundsätzen des Datenschutzes durch Technik** (data protection by design) und durch **datenschutzfreundliche Voreinstellungen** (data protection by default) Genüge tun. Erreicht werden kann dies nur durch frühzeitiges Handeln.

## a) Organisations- und Strukturprojekte

Die folgende Liste gibt einen nicht abschließenden Überblick über Vorhaben und Projekte im NDR, in denen sich der oben skizzierte Handlungsbedarf entfaltete:

- Beachtung von Anforderungen des Datenschutzes in Auslandsstudios
- Einführung von Eventplanungssystemen
- Anwendungen für Gästemanagementtools, Einladungs- und Teilnehmermanagementsysteme
- Community-Management-Tools
- Ersatz von Systemen zur Medienproduktion
- Systeme für Klangkörper-Verwaltungen und Einsätze
- Systemanpassungen bei Ausspielwegen
- Management in der Vernetzten Produktion
- Webanwendungen für die Publikation von Videos
- Bereitstellung von Bildmaterialtools-Tool
- Agenturmonitoring im Bereich ARD-Aktuell
- Bereitstellung eines Open-Source-Whistleblower-Einreichungssystems für investigative Zwecke
- Einführung einer Crossmediale Suche
- Interne Suchmaschinen
- Einrichtung eines Interviewtools
- Anpassungen bei Sendeabwicklungen
- Druckkonzepte
- Beschaffung von Übertragungswagen
- Ersatz von Audiotechnik
- Modernisierung von Studios
- Anpassungen bei Sendeabwicklungen
- Ausstattung von Arbeitsplätzen
- Rahmenbedingungen von Produktivzeiterfassungen
- Arbeitszeitaufschreibung für Aushilfen und Studierende
- Gestaltung und Bereitstellung von Dienstplänen
- Mobilisierung von Webanwendungen für Beschäftigte

- Weiterentwicklung und Einführung von Kollaborationssystemen
- Digitale Unfallmeldesysteme
- Errichtung des Crossmediales Nachrichtenhauses
- Maßnahmen zum Schutz der Daten und Einrichtungen des NDR vor der Nutzung durch suspendierte Personen
- technische Umsetzung Desksharing und hybrides Arbeiten
- Telefonkonzepte für neue Standard IT-Arbeitsplätze

Auch die Nutzung von Microsoft-365-Anwendungen löst ständigen Befassungsaufwand aus. Beraten wird hier insbesondere ein **Datenschutz- und IT-Sicherheitskonzept**, das aufgrund der Dynamik der Anwendungen weiterentwickelt werden muss.

Überdies wurden über 100 Prüfungen von IT-Systemen und kleineren Softwareanwendungen, Apps und sonstigen digitalen Anwendungen vorgenommen.

## b) Datensicherheit

Im Tätigkeitsbericht für das Jahr 2021 wurde an dieser Stelle umfangreich auf generelle und konkrete Gefahren für die Daten- und IT-Sicherheit eingegangen. Für das Jahr 2022 fällt dieser Berichtspunkt kürzer aus. Dies jedoch nicht, weil die Gefahren geringer geworden sind. Im Gegenteil: Die Berichterstattung über entsprechende Sicherheitsvorfälle und Angriffe auf Unternehmen und Behörden ist alltäglich geworden und die Gefahren sind mithin bekannt. **Die Kehrseite der Digitalisierung von privaten und geschäftlichen Vorgängen ist eine Gefahrenlage, die aus vermehrten Cyber-Angriffen resultiert.** Nicht zuletzt sind derartige Angriffe auch Bestandteil kriegerischer Auseinandersetzungen. Erforderlich sind daher organisatorische und technische Maßnahmen, um den Schutz der Daten- und IT-Sicherheit zu erhöhen. Der NDR hat entsprechende Maßnahmen ergriffen, technische Systeme ausgebaut und das Monitoring zur Erkennung von Angriffen erhöht. Weiterhin wurden Achtsamkeitskampagnen ins Leben gerufen, um mehr Aufmerksamkeit auf verdächtige Kommunikationsversuche und Zuschriften zu lenken, da

insbesondere sogenannte Phishing-Mails Cyberangriffe mit hohem Schadenspotential bedeuten können.

#### **F. Anfragen nach dem Informationszugang**

Seit September 2021 können Informationsfreiheitsansprüche an den NDR gerichtet werden (§ 47 NDR Staatsvertrag). Beschwerdestelle ist der Rundfunkdatenschutzbeauftragte für den Fall, dass Antragstellende, die der Ansicht sind, dass ein Informationsanspruch zu Unrecht abgelehnt, nicht beachtet oder nur unzulänglich beantwortet ist, die Rückmeldung des NDR überprüfen lassen wollen. Im Berichtsjahr wurden 6 Ansprüche an den NDR gerichtet. Diese führten allerdings nicht zu Beschwerden. Die Tätigkeit des Rundfunkdatenschutzbeauftragten war daher beschränkt auf punktuelle Anfragen zu einzelnen Modalitäten der Auskunftserteilung.

## G. Fazit und Ausblick

Digitalisierungsprozesse werden gesamtgesellschaftlich und damit auch im NDR und seinen Beteiligungsunternehmen weiterhin eine gewichtige Rolle einnehmen. Die Vorteile dieser Entwicklungen liegen auf der Hand, gleiches gilt jedoch auch für die Gefahren. Die Selbstverständlichkeit im Umgang mit digitalisierten Prozessen und das mit einhergehende Vertrauen in deren Stabilität und Funktionalität birgt Risiken. Die Anforderungen des Datenschutzes sollen die Prozesse gestalten und begleiten und die Risiken zumindest minimieren, bestenfalls eliminieren.

Alle Gesellschaften sind anhaltenden Revolutionen der Informationstechnologien ausgesetzt. Es gibt Warnungen, dass Digitalisierungsprozesse Diktaturen effizienter machen können als demokratisch verfasste Gesellschaften. Grund dafür sei, dass zentralisierte, staatliche Datenverarbeitungssysteme weitaus wirksamer eingesetzt werden als dezentrale: „Der Kapitalismus habe den Kommunismus denn auch deshalb besiegt, weil er in seiner Datenverarbeitung effizienter gewesen sei. Ebenso seien die Systeme von Demokratie und Diktatur letztlich Datenverarbeitungssysteme: «Da sowohl Menge als auch Geschwindigkeit der Daten zunehmen, könnten altehrwürdige Institutionen wie Wahlen, Parteien und Parlamente obsolet werden – nicht weil sie unmoralisch wären, sondern weil sie die Daten nicht effizient genug verarbeiten.» (Zitat von Yuval Noah Harari, zu finden unter <https://www.nzz.ch/leserdebatte/was-glauben-sie-foerdert-die-digitalisierung-die-diktatur-ld.1384094>).

Der öffentlich-rechtliche Rundfunk ist seit jeher Bestandteil der demokratischen Verfassung. Als solcher muss er im fortwährenden Prozess der Digitalisierung in seiner eigenen Verfasstheit und seiner gesellschaftlichen Rolle – gerade auch wegen der Abwesenheit ökonomischer Interessen – die digitalen Transformationen unter Berücksichtigung der Rechts auf informationelle Selbstbestimmung begleiten und mitgestalten. Denn:

„Digitalisierung ohne Datenschutz ist wie die Entwicklung eines Medikamentes ohne Prüfung auf Nebenwirkung“

([https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2018/11\\_DigitalisierungUndDatenschutz.html](https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2018/11_DigitalisierungUndDatenschutz.html)).