NORDDEUTSCHER RUNDFUNK

Tätigkeitsbericht des Rundfunkdatenschutz-beauftragten

für das Berichtsjahr 2018

Dr. Heiko Neuhoff

Hamburg im Februar 2019

Vorgelegt wird hiermit der Bericht gemäß § 4 Abs. 4 NDR-Datenschutz-Staatsvertrag i. V. m. Artikel 59 der Verordnung (EU) 2016/679 (DSGVO) über die Tätigkeit des Rundfunkdatenschutzbeauftragten des NDR.

Danksagung

Im Sekretariat des (Rundfunk-) Datenschutzbeauftragten hat Frau Susanne Korpys bis zum 24. Mai 2018 gearbeitet. Am 1. Oktober 2018 hat Frau Heike Ramand diese Aufgabe übernommen. Frau Cornelia Weitzel-Kerber war stellvertretende Datenschutzbeauftragte des NDR und hat dieses Amt zum 25. Mai 2018 niedergelegt. Allen sei herzlich für die geleistete Arbeit und die Unterstützung bei den Erledigungen der Aufgaben und der Erstellung dieses Berichts gedankt.

Inhalt

Teil A – Bericht 5

A. Zusammenfassung der wesentlichen Ergebnisse 5

B. Rechtsgrundlagen der Tätigkeit des NDR (Rundfunk-) Datenschutzbeauftragten 5

C. Personalien 6

D. Wesentliche (rechtliche) Entwicklungen im Berichtszeitraum 6

I. Gesetzgebung 7

1. Datenschutzgrundverordnung 8

2. NDR-Datenschutz-Staatsvertrag und Rundfunkstaatsvertrag 9

3. Bundesdatenschutzgesetz 13

4. Zukünftige Gesetzgebungen, e-Privacy-Verordnung 14

5. Entwurf eines Gesetzes zum Schutz von Geschäftsgeheimnissen 15

II. Rechtsprechung 15

1. EuGH-Urteil zur gemeinsamen Verantwortlichkeit beim Betrieb einer Facebook-Fanpage 16

2. BGH-Urteil vom 17.05.2018 zur Vererbbarkeit von Facebook-Nutzerkonten 17

3. Abmahnfähigkeit von Datenschutz-Verstößen 18

4. Anwendbarkeit des KUG 19

E. Tätigkeiten des (Rundfunk-) Datenschutzbeauftragten im Berichtszeitraum 20

I. Umsetzung der DSGVO 25

1. Anpassungen der Datenschutzerklärungen 25

2. Veröffentlichung der proaktiven Informationen nach Art. 13 DSGVO 26

3. Gewinnspiele, Hinweise bei Sprachassistenten und Nutzungen von Drittplattformen 30

4. Organisation eines Verfahrens zur Beauskunftung von Anfragen gemäß Art. 15 DSGVO 31

5. Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) 32

6. Etablierung eines Verfahrens zur Datenschutzfolgeabschätzung nach Art. 35 DSGVO 32

7. Kameraüberwachungen 33

8. Auftragsverarbeitungen 34

9. Anpassung sonstiger Verträge und Muster 35

II. Redaktionsdatenschutz/Redaktionsgeheimnis 35

III. Rundfunkteilnehmerdatenverwaltung 37

IV. Personaldatenverwaltung 41

V. Sonstige Informationen 43

VI. Organisations- und Strukturprojekte 45

VII. Verbreitungsfragen 47
VIII. Zusammenarbeit mit anderen Datenschutzbeauftragten 49
1. AKDSB 49
2. Das virtuelle Datenschutzbüro 50
3. Zusammenarbeit mit anderen Aufsichtsbehörden auf nationaler Ebene 50
F. Ausblick 52
Teil B – Anlagen: Auszüge aus wesentlichen gesetzlichen Grundlagen 53

Teil A – Bericht

A. Zusammenfassung der wesentlichen Ergebnisse

Das Berichtsjahr war maßgeblich geprägt durch die Umsetzung der Datenschutzgrundverordnung. In allen Bereichen des Norddeutschen Rundfunks waren Umstellungs- und Anpassungsmaßnahmen notwendig. Insgesamt kann festgehalten werden, dass die erforderlichen Maßnahmen erfolgreich umgesetzt werden konnten. Vorab kann zudem zusammenfassend Folgendes mitgeteilt werden:

- Es gab im Jahr 2018 keinen Anlass für den (Rundfunk-) Datenschutzbeauftragten, eine förmliche Beanstandung auszusprechen.
- Die Anzahl der zu prüfenden Projekte und Vorhaben ist nennenswert angestiegen. Aufgrund der gesetzlichen Änderungen, namentlich insbesondere der Geltung der Datenschutzgrundverordnung (DSGVO) und des NDR-Datenschutz-Staatsvertrages ab dem 25. Mai 2018, hat sich auch die Anzahl der Schulungen und Beratungen deutlich erhöht.
- Wohl auch aufgrund der in der Medienöffentlichkeit verbreiteten thematisierten Geltung der DSGVO und dem in dieser Verordnung geregelten Auskunftsanspruch ist die Anzahl von Auskunftsersuchen und Eingaben erheblich gestiegen.
- Eine externe datenschutzrechtliche Prüfung wurde bei einem Auftragsverarbeiter des NDR vorgenommen. Bei einer weiteren externen datenschutzrechtlichen Prüfung beim Informations- und Verarbeitungszentrum (IVZ) konnte der Verfasser dieses Berichts leider nicht teilnehmen.

B. Rechtsgrundlagen der Tätigkeit des NDR (Rundfunk-) Datenschutzbeauftragten

Rechtsgrundlage für die Tätigkeit des (Rundfunk-) Datenschutzbeauftragten des NDR war bis zum 24. Mai 2018 der NDR Staatsvertrag in seiner seit dem 01. August 2005 geltenden Fassung. Am 25. Mai 2018 trat die DSGVO endgültig in Kraft. Gleiches gilt für den NDR-Datenschutz-Staatsvertrag, der insoweit die einschlägigen Regelungen des NDR Staatsvertrags außer Kraft setzte. Der Datenschutzbeauftragte des NDR war bis zum 24. Mai 2018 gemäß der Datenschutzrichtlinie datenschutzrechtliche Kontrollstelle gemäß Art. 28 (Richtlinie 95/46/EG) und ist seitdem Aufsichtsbehörde nach Art. 51 DSGVO. Einschlägige Rechtsgrundlagen bzw. Auszüge daraus sind als **Anlage** diesem Bericht beigefügt.

C. Personalien

Der Verfasser dieses Berichts wurde vom Rundfunkrat des NDR für die Dauer von 4 Jahren ab dem 25. Mai 2018 zum Rundfunkdatenschutzbeauftragten auf Vorschlag des NDR Verwaltungsrats ernannt. Zuvor hatte der Verfasser das Amt des Datenschutzbeauftragten des NDR seit dem 1. September 2017 inne. Aufgrund der Vorgabe des § 2 Abs. 2 S. 5 NDR-Datenschutz-Staatsvertrag kann das Amt des Rundfunkdatenschutzbeauftragten seit dem 25. Mai 2018 nur hauptamtlich ausgeübt werden. Seit dem 1. Oktober 2018 unterstützt Frau Heike Ramand den Rundfunkdatenschutzbeauftragten.

Frau Cornelia Weitzel-Kerber hat ihr Amt als stellvertretende Datenschutzbeauftragte des NDR zum 25. Mai 2018 niedergelegt.

In der Sitzung des Arbeitskreises der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio (AKDSB) am 8./9. November 2018 wurde der Verfasser zum Vorsitzenden des AKDSB ab dem 1. Januar 2019 gewählt.

D. Wesentliche (rechtliche) Entwicklungen im Berichtszeitraum

„Datenschutz und Privatsphäre werden in allen Ländern der Welt ein Topthema werden. Ich glaube, dieser Komplex gehört zu den zwei oder drei wichtigsten Themen dieses Jahrhunderts." Dieses Zitat und auch die Aussage, dass Datenschutz ein Kernprinzip sei, an dem sich alle Entwicklungen des Unternehmens orientieren würden, entstammt nicht etwa einem praxisfernen Optimisten. Vielmehr hat Apple-Chef Tim Cook sich derart auf der 40. Internationalen Konferenz der Datenschutzbeauftragten in Brüssel geäußert. Seiner Meinung nach sei die DSGVO „ein Beispiel dafür, wie gute Grundsätze und politischer Wille zusammenkommen, um unser aller Rechte zu verteidigen".

Die Datenschutzgrundverordnung hat also über ihren Geltungsbereich hinaus Beachtung und sogar Anerkennung gefunden. Und auch insgesamt ist eine gesteigerte Sensibilität und ein gewachsenes Bewusstsein für datenschutzrechtliche Belange zu verzeichnen: Während der Erstellung dieses Berichts wurde eine Umfrage von Infratest Dimap für den ARD-DeutschlandTrend auf tagesschau.de veröffentlicht. Darin heißt es: „Die Deutschen sind mehrheitlich eher vorsichtig, wenn sie im Internet unterwegs sind: 60 Prozent versuchen, online so wenige persönliche Daten wie möglich anzugeben - auch wenn sie deshalb manche Dienste nicht nutzen können. 37 Prozent hingegen sagen, dass sie persönliche Daten

angeben, wenn es für die Nutzung bestimmter Dienste erforderlich ist. Nur drei Prozent geben an, dass sie die Weitergabe persönlicher Daten im Internet unproblematisch finden. […]. Entsprechend groß ist die Sorge der Internetnutzer, ihre persönlichen Daten könnten missbraucht werden. Eine Mehrheit von 61 Prozent der Befragten macht sich in diesem Zusammenhang große oder sogar sehr große Sorgen. Anders sehen das 35 Prozent der Deutschen: Sie machen sich nur geringe Sorgen, vier Prozent haben gar keine Angst vor Datenmissbrauch. Auffällig ist, dass die junge Generation von 18 bis 34 Jahren offenbar weniger Sorge vor Datenmissbrauch hat. Hier macht sich eine Mehrheit von 51 Prozent eine geringe oder gar keine Sorge um den Missbrauch persönlicher Daten“ (https://www.tagesschau.de/inland/deutschlandtrend/index.html, abgerufen am 11.01.2019).

Ein Bewusstsein für den Schutz personenbezogener Daten ist mithin vorhanden. Gleiches gilt auch für geeignete Maßnahmen für den Schutz vor Datenmissbrauch: „Dazu gaben 90 Prozent der befragten Internetnutzer an, dass sie niemals E-Mail-Anhänge von unbekannten Absendern öffnen würden. 83 Prozent sagen, dass sie regelmäßig Software-Updates auf Computern oder Smartphones installieren. Eine Mehrheit (56 Prozent) gab an, dass sie keine öffentlichen WLAN-Hotspots verwenden. Gefragt zur Zwei-Faktor-Authentifizierung, die sowohl bei Online-Banking als auch teilweise bei E-Maildiensten und anderen Internet-Anwendungen verwendet wird, sagen 46 Prozent der Befragten, dass sie häufig diese Form nutzen würden. 40 Prozent sagen, dass sie mindestens alle paar Monate die Passwörter ihrer Online-Zugänge erneuern würden.“

Wesentlich für das gesteigerte Bewusstsein für datenschutzrechtliche Belange dürfte dabei u. a. gewesen sein, dass das Jahr 2018 für Facebook das wohl schwierigste Jahr bislang darstellte, da im März 2018 bekannt geworden war, dass sich die britische Analysefirma Cambridge Analytica Zugang zu Daten von 87 Millionen Nutzer*innen von Facebook verschafft hatte.

I. Gesetzgebung

Wie eingangs unter B. erwähnt, haben sich im Berichtsjahr 2018 die datenschutzrechtlichen Grundlagen wesentlich erneuert. Das Datenschutzrecht wurde durch die Datenschutzgrundverordnung reformiert und in den Mitgliedstaaten vereinheitlicht. Als sogenannte „hinkende Verordnung“ sieht die DSGVO Öffnungsklauseln vor, um den nationalen Gesetzgebern Raum für eine weitergehende Regulierung zu geben. Mit dem NDR-Datenschutz-Staatsvertrag und auch Anpassungen im Rundfunkstaatsvertrag hat der

Landesgesetzgeber diese Möglichkeiten genutzt. Zudem hat auch der Bundesgesetzgeber im Rahmen seiner Kompetenz Anpassungen vorgenommen. Nur soweit der NDR betroffen ist, wird aufgrund der Vielzahl der Novellierungen auf die gesetzgeberische Tätigkeit eingegangen. Andernfalls würde der Rahmen dieses Berichts gesprengt werden.

1. Datenschutzgrundverordnung

Mit Geltung der Datenschutzgrundverordnung (VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO)) zum 25. Mai 2018 wurde gemäß Art. 94 Abs. 1 DSGVO die Richtlinie 95/46/EG aufgehoben. Aufgrund der in der DSGVO normierten Öffnungsklauseln für Mitgliedstaaten (Art. 85 DSGVO) konnte der nationale Gesetzgeber für besondere Verarbeitungssituationen Abweichungen und Ausnahmen von der DSGVO vorsehen. Der Gesetzgeber der vier Staatsvertragsländer des NDR hat daher den Staatsvertrag über den Datenschutz beim Norddeutschen Rundfunk (NDR-Datenschutz-Staatsvertrag) ebenfalls zum 25. Mai 2018 in Kraft gesetzt. Zugleich haben die Bundesländer durch den 21. Rundfunkänderungsstaatsvertrag erforderliche Anpassungen vorgenommen, um insbesondere journalistisches Arbeiten weiterhin möglich zu machen.

Die Datenschutzgrundverordnung hat im Wesentlichen den materiell-datenschutzrechtlichen Regelungsgehalt zuvor bestehender deutscher Regulierungen beibehalten, aber neu definiert und erweitert. Neue Transparenz- und Dokumentationsverpflichtungen führen nun zu erhöhtem Verwaltungsaufwand der Verantwortlichen und der Aufsichtsbehörden.

Den Verantwortlichen (NDR) treffen beispielsweise nun proaktive Informationspflichten gemäß Art. 13 DSGVO bei Datenerhebung über z.B.

- Kontaktdaten des NDR und des Rundfunkdatenschutzbeauftragten,
- die Zwecke und die Rechtsgrundlagen der Datenverarbeitungen,
- Auftragsverarbeiter des NDR,
- etwaige Absichten der Datenübermittlung in ein Drittland,
- Speicherdauern von personenbezogenen Daten sowie

- Hinweispflichten auf Betroffenenrechte inklusive der Möglichkeit einer Beschwerde beim Rundfunkdatenschutzbeauftragten.

Gleiches gilt bezüglich der Dokumentationspflichten: Der NDR muss nachweisen können, dass er Daten rechtmäßig verarbeitet (sog. Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO). Dies etwa durch

- ein Verzeichnis für Verarbeitungstätigkeiten (Art. 30 DSGVO),
- Nachweise über wirksam eingeholte Einwilligungen,
- technisch-organisatorische Maßnahmen (Art. 24 DSGVO),
- die Dokumentation von Datenschutzvorfällen (Art. 33 Abs. 5 DSGVO),
- die Sicherstellung der Betroffenenrechte (Auskunftserteilung, Mitteilung der Berichtigung, Löschung usw.).

Neu durch die DSGVO hinzugekommen ist auch die Datenschutzfolgenabschätzung. Dies ist ein Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Durchzuführen ist ein solches Verfahren, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat.

Sämtliche von der DSGVO eingeführte Neuerungen können an dieser Stelle nicht beschrieben werden. Sie sind aber den folgenden Ausführungen zu entnehmen.

2. NDR-Datenschutz-Staatsvertrag und Rundfunkstaatsvertrag

Im NDR-Datenschutz-Staatvertrag wird insbesondere die Stellung und Ausformung der datenschutzrechtlichen Aufsichtsbehörde über den NDR konkretisiert. In der Praxis besteht diese Behörde nach Art. 51 DSGVO aus einem hauptamtlichen Rundfunkdatenschutzbeauftragten und einer Mitarbeiterin (s. C. – Personalien).

§ 2 NDR-Datenschutz-Staatsvertrag regelt die Voraussetzungen der Ernennung der oder des Rundfunkdatenschutzbeauftragten und bestimmt die Amtszeit. In § 3 wird die Unabhängigkeit der oder des Rundfunkdatenschutzbeauftragten normiert. § 4 beschreibt die Aufgaben und Befugnisse. Auf der Grundlage des § 2 Abs. 3 NDR-

Datenschutz-Staatsvertrag hat der NDR Verwaltungsrat mit Beschluss vom 18.05.2018 und mit Zustimmung des NDR Rundfunkrates vom 25.05.2018 eine Satzung über die oder den Rundfunkdatenschutzbeauftragte/n beim Norddeutschen Rundfunk erlassen. Kern dieser Satzung ist die Konkretisierung der Beschreibung der Aufgaben der/des Rundfunkdatenschutzbeauftragten. Diese sind gemäß Art. 2 der Satzung:

- die Anwendung der Vorschriften über den Datenschutz zu überwachen und durchzusetzen;
- die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;
- im Einklang mit dem geltenden Recht den NDR, seine Hilfs- und Beteiligungsunternehmen und Gremien über Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten;
- die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten zu sensibilisieren;
- auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund der Vorschriften über den Datenschutz zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit anderen Aufsichtsbehörden zusammenzuarbeiten;
- sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
- mit anderen Aufsichtsbehörden unter Wahrung der medienfreiheitimmanenten Grenzen zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung der Vorschriften über Datenschutz zu gewährleisten;
- Untersuchungen über die Anwendung der DSGVO durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

- maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;
- Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 DSGVO und des Artikels 46 Absatz 2 Buchstabe d DSGVO festzulegen;
- eine Liste der Verarbeitungsarten zu erstellen und zu führen, für die gemäß Artikel 35 Absatz 4 DSGVO eine Datenschutzfolgenabschätzung durchzuführen ist;
- Beratung in Bezug auf die in Artikel 36 Absatz 2 DSGVO genannten Verarbeitungsvorgänge zu leisten;
- die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 DSGVO zu fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 DSGVO bieten müssen, Stellungnahmen abzugeben und sie zu billigen;
- Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 DSGVO zu genehmigen;
- verbindliche interne Vorschriften gemäß Artikel 47 DSGVO zu genehmigen;
- interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 DSGVO ergriffene Maßnahmen zu erstellen und jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten zu erfüllen.

§ 1 NDR-Datenschutz-Staatsvertrag und § 9c RStV regeln die Datenverarbeitung zu journalistischen Zwecken und damit das sogenannte Medienprivileg. Dieses Medienprivileg schafft notwendige Ausnahmen von datenschutzrechtlichen Grundsätzen, namentlich dem Erfordernis einer Einwilligung oder das Vorliegen einer Rechtsgrundlage zur Verarbeitung personenbezogenen Daten, um die redaktionelle Arbeit weiterhin zu ermöglichen. Mit den beiden genannten Paragraphen hat der Gesetzgeber von der gemäß Art. 85 DSGVO eröffneten Möglichkeit Gebrauch gemacht und „durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken in Einklang“ gebracht. In der Begründung des Gesetzgebers des Rundfunkstaatsvertrages heißt es diesbezüglich:

„Die Mitgliedstaaten sind also in der Form eines Abwägungsgebotes verpflichtet, einen angemessenen Ausgleich zwischen dem Schutz personenbezogener Daten und dem Recht auf freie Meinungsäußerung und auf Informationsfreiheit zu schaffen. Dies umfasst insbesondere die hinsichtlich der bei Recherche und Vorbereitung von

Publikationen unverzichtbare Befugnis zur Verarbeitung personenbezogener Daten auch ohne Einwilligung des Betroffenen, den Ausschluss von Auskunfts- und Berichtigungsansprüchen betroffener Personen und das Fehlen einer staatlichen datenschutzrechtlichen Aufsicht. Die Ausnahmen und Beschränkungen sind bisher und auch zukünftig aufgrund der herausragenden Bedeutung freier, keiner staatlichen Kontrolle unterworfener Medien für die öffentliche Meinungsbildung und die Meinungsvielfalt in einem demokratischen System und ihrer unerlässlichen Kontrollaufgabe („Wächteramt“) geboten und gerechtfertigt. Ohne die Verarbeitung personenbezogener Daten auch ohne Einwilligung der jeweils betroffenen Personen wäre journalistische Arbeit nicht möglich und die Presse könnte ihre in Artikel 5 Abs. 1 Satz 2 des Grundgesetzes, Artikel 10 Abs. 1 Satz 2 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten sowie Artikel 11 Abs. 1 Satz 1 der Charta der Grundrechte der Europäischen Union zuerkannten und garantierten Aufgaben nicht wahrnehmen (vgl. BVerwG, Beschluss vom 29. Oktober 2015 – 1 B 32/15, Rdnr. 5, m.w.N.). Die Abwägungsentscheidung zwischen den widerstreitenden Grundrechtspositionen der informationellen Selbstbestimmung (Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes) einerseits und der Meinungs-, der Informations- und den Medienfreiheiten (Artikel 5 Abs. 1 S. 1 und 2 des Grundgesetzes) andererseits wurde bereits im Rahmen der bestehenden datenschutzrechtlichen Regelungen vorgenommen. Diese Abwägungsentscheidung wurde im Lichte der Datenschutzgrundverordnung einer erneuten Überprüfung unterzogen, insbesondere auch im Hinblick auf den Schutz personenbezogener Daten und der Meinungs- und Medienfreiheit gemäß der Artikel 8 und 11 der Charta der Grundrechte der Europäischen Union. Die Untersuchung führte allerdings zu keinen erheblichen Veränderungen bei der Gewichtung der einzelnen Positionen.

Die in den rundfunkrechtlichen Staatsverträgen vorgenommenen Änderungen beschränken sich daher auf Anpassungen, deren Notwendigkeit sich durch die Verabschiedung der Datenschutzgrundverordnung ergeben. Von den in der Verordnung enthaltenen Regelungsermächtigungen wurde umfangreich Gebrauch gemacht, ohne den insbesondere durch Artikel 85 der Datenschutzgrundverordnung eingeräumten Umsetzungsspielraum zu überschreiten. Die Möglichkeit, weitgehend an bewährten Strukturen festzuhalten, entspricht nach der Entstehungsgeschichte von Artikel 85 Abs. 1 und 2 auch der Intention des europäischen Gesetzgebers. Im Medienbereich wird so ein einheitliches, angemessenes und ausgewogenes Datenschutzniveau gewährleistet, das für die betroffene Person zudem durch den zivilrechtlichen Persönlichkeitsrechtsschutz flankiert wird.“

Für den NDR ist das Medienprivileg wesentliche Voraussetzung für die Erfüllung des Programmauftrags. Nur durch das Medienprivileg werden die Informationsrechte gewährleistet, die der NDR und alle anderen Medien für die Erfüllung ihrer Funktion der Meinungsbildung benötigen. Zugleich stellt es ein Instrument dar, damit Medien vor staatlichen Zugriffen geschützt werden. Weiterhin bewahrt es davor, dass von einer Berichterstattung Betroffene diese Berichterstattung über sonstige allgemeine zivil- und strafrechtliche Ansprüche unterbinden können, ohne dass zuvor eine Abwägung zwischen Persönlichkeitsrechten mit Kommunikationsfreiheiten der Medien stattgefunden hat.

3. Bundesdatenschutzgesetz

Die DSGVO hat in Deutschland regen Bedarf an Gesetzesanpassungen ausgelöst. Mit dem Zweiten Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) hat der Bundesgesetzgeber z. B. die Erforderlichkeit der Novellierung von 155 Bundesgesetzen erkannt. Im besonderen Maße relevant für den NDR sind Neuerungen im Bundesdatenschutzgesetz (BDSG), da in § 26 BDSG die Vorgaben der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses gefasst wurden. Danach gilt nun:

- Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

- Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.
- Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Absatz 2 gilt entsprechend.
- Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.
- Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.
- Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

4. Zukünftige Gesetzgebungen, e-Privacy-Verordnung

Der europäische Gesetzgeber hatte beabsichtigt, am 25. Mai 2018 die sogenannte e-Privacy-Verordnung (VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RA-

TES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)) in Kraft zu setzen. Dies ist jedoch nicht erfolgt. Zudem ist auch unklar, wann und mit welchem genauen Wortlaut diese Verordnung erlassen wird. Relevant kann eine e-Privacy-Verordnung etwa für die Telemedienangebote des NDR werden.

Aufgrund Art. 97 DSGVO steht fest, dass die Datenschutzgrundverordnung bis zum 25. Mai 2020, und danach alle vier Jahre, evaluiert werden soll.

Weitere gesetzgeberische Tätigkeit ist – nicht zuletzt wegen der fortschreitenden Digitalisierung – auch auf nationaler Ebene zu erwarten. Noch nicht absehbar ist etwa, ob es – wie im Koalitionsvertrag zwischen CDU, CSU und SPD vom 07. Februar 2018 angedacht – zu einem eigenständigen Gesetz zum Beschäftigtendatenschutz kommen wird.

5. Entwurf eines Gesetzes zum Schutz von Geschäftsgeheimnissen

Die Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung soll durch ein neues Gesetz in nationales Recht umgesetzt werden. Ziel ist der Schutz vor rechtswidriger Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen.

Wesentlich wird dabei sein, ob es gelingt, die journalistische Tätigkeit – einschließlich der Hinweisgeber zu schützen.

Derzeit wird der Gesetzentwurf im parlamentarischen Verfahren beraten.

II. Rechtsprechung

Anbei wird eine Auswahl von für den NDR wesentlichen Entscheidungen des Jahres 2018 aus dem Datenschutzrecht vorgestellt.

1. EuGH-Urteil zur gemeinsamen Verantwortlichkeit beim Betrieb einer Facebook-Fanpage

Dem EuGH-Urteil vom 05. Juni 2018 war ein Verfahren um die datenschutzrechtliche Verantwortung für die anonymisierten und statistischen Daten, die durch die Funktion „Facebook Inside“ erhoben würden, vorausgegangen. Der Europäische Gerichtshof hat nun geurteilt, dass sowohl Facebook als auch der Betreiber einer Facebook-Seite verantwortlich seien. Die gemeinsame Verantwortlichkeit sei aber nicht gleichbedeutend mit einer gleichwertigen Verantwortlichkeit. Deshalb ist die Frage, wie sich diese Verantwortung aufteilt und wer bei Verstößen zur Verantwortung gezogen werden kann, wiederum durch das Bundesverwaltungsgericht (BVerwG) zu klären. Wann das BVerwG über die Umsetzung der Vorgaben des EuGH entscheiden wird, steht noch nicht fest.

Der NDR hat aufgrund des EuGH-Urteils seine Datenschutzerklärung angepasst. Dort heißt es diesbezüglich:

„Präsenzen auf Drittplattformen
Der NDR betreibt Präsenzen auf Drittplattformen, deren Betreiber Daten ihrer Nutzerinnen und Nutzern verarbeiten und speichern. Auf deren datenschutzrechtlichen Bestimmungen und Einstellungen hat der NDR leider keinen Einfluss. Ausdrücklich wird darauf hingewiesen, dass die Drittplattformen auch Cookies setzen, mit denen sie das Nutzungsverhalten auf anderen Webseiten und Apps des Konzerns verfolgen können sowie auf bestimmten Webseiten und Apps, die Technologien dieser Drittplattform integrieren. Informationen über die erhobenen Daten und ihre Verwendung, den Zweck der Speicherung, Lösch- und Auskunftsersuchen sind in den Datenschutzhinweisen der jeweiligen Plattform festgehalten.“

Neben diesem Hinweis in der Datenschutzerklärung des NDR auf die jeweiligen Datenschutzbestimmungen von Drittplattformen wurden folgende Maßnahmen ergriffen:

- Gesonderte Hinweise auf den Facebook-Profilen, dass der NDR auf die datenschutzrechtlichen Bestimmungen dieser Plattform sowie auf die Erhebung, Analyse und Nutzung von User-Daten keinen Einfluss hat.

- Hinweise auf allen Facebook-Präsenzen des NDR, dass NutzerInnen von Facebook eine Kopie der eigenen Daten einsehen können und die Datenschutzeinstellungen dort nutzen sollten. Außerdem wird dort auf die Datenschutzerklärung des NDR aufmerksam gemacht.
- Regelmäßige Hinweise im Programm des NDR, von den Datenschutzeinstellungen auf Facebook Gebrauch zu machen.

Aufgrund der gemeinsamen Verantwortlichkeit von Facebook und dem Betreiber einer Fanpage ist es zudem notwendig, eine Vereinbarung über die Wahrnehmung der Verpflichtungen gemäß Art. 26 DSGVO zu schließen. Auf der „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ hat Facebook zwar aufgrund des Urteils erklärt: „Facebook Ireland stimmt zu, die primäre Verantwortung gemäß DSGVO für die Verarbeitung von Insights-Daten zu übernehmen und sämtliche Pflichten aus der DSGVO im Hinblick auf die Verarbeitung von Insights-Daten zu erfüllen (u. a. Artikel 12 und 13 DSGVO, Artikel 15 bis 22 DSGVO und Artikel 32 bis 34 DSGVO). Darüber hinaus wird Facebook Ireland das Wesentliche dieser Seiten-Insights-Ergänzung den betroffenen Personen zur Verfügung stellen.“ Damit übernimmt Facebook Ireland die primäre Verantwortung für die Verarbeitung von Insights-Daten. Gleichwohl wird der NDR (und andere (Rundfunkanstalten) auch) mit Facebook eine Vereinbarung nach Art. 26 DSGVO schließen müssen.

2. BGH-Urteil vom 17.05.2018 zur Vererbbarkeit von Facebook-Nutzerkonten

Der Bundesgerichtshof hat bezüglich der Frage zum „digitalen Nachlass“ entschieden, dass Erben Zugang zu dem Facebook-Benutzerkonto einer Erblasserin sowie den darin enthaltenen Inhalten gewährt werden muss. Erben haben damit gegen Facebook und andere vergleichbare Plattformen einen Anspruch, die in dem Account vorgehaltenen Kommunikationsinhalte einzusehen. Ein schutzwürdiges Vertrauen darauf, dass nur der Kontoinhaber und nicht Dritte von dem Kontoinhalt Kenntnis erlangen, bestehe nicht. Auch scheide eine Differenzierung des Kontozugangs nach vermögenswerten und höchstpersönlichen Inhalten aus. Nach der gesetzgeberischen Wertung gehen auch Rechtspositionen mit höchstpersönlichen Inhalten wie Tagebücher und persönliche Briefe auf die Erben über. Digitale Inhalte seien ebenso zu behandeln. Der Anspruch auf Zugang zu dem Konto kollidiere auch nicht mit datenschutzrechtlichen Vorgaben. Der BGH hatte zur Entscheidungsfindung die Datenschutzgrundverordnung anzuwenden und befunden, dass diese dem Zugang der Er-

ben nicht entgegenstehe. Datenschutzrechtliche Belange von Erblassern seien nicht betroffen, da die Verordnung nur lebende Personen schütze.

Mit diesem Urteil zum digitalen Nachlass gleicht der BGH analoge Schriftstücke und (private) E-Mail- und Social-Media-Accounts erbrechtlich an. Bedeutung können derartige Sachverhalte in unterschiedlichen Konstellationen erlangen. Ob dazu noch gesetzgeberisches Handeln folgt, ist derzeit unklar. Der aktuelle Koalitionsvertrag führt dazu aus: „Wir werden die Vererbbarkeit des digitalen Eigentums (z. B. Nutzeraccounts, Datenbestände) rechtssicher gesetzlich regeln“ (Randnummern 6204, 6205).

3. Abmahnfähigkeit von Datenschutz-Verstößen

Unterschiedlich haben deutsche Gerichten bislang zur Abmahnfähigkeit von Datenschutz-Verstößen entschieden. Eine höchstrichterliche Entscheidung steht noch aus. Das OLG Hamburg (Urteil vom 25. Oktober 2018, Az.: 3 U 66/17) und das LG Würzburg (Beschluss vom 13. September 2018, Az.: 11 O 1741/18 UWG) haben zu Gunsten der Abmahnfähigkeit von Datenschutzverstößen entschieden (anders hingegen das LG Bochum (Urteil vom 7. August 2018, Az.: I-12 O 85/18). Das OLG Hamburg und das LG Würzburg sind der Auffassung, dass Verstöße gegen datenschutzrechtliche Pflichten abmahnfähig sind. Das bedeutet, dass etwa eine nicht den Anforderungen der DSGVO entsprechende Datenschutzerklärung einen abmahnfähigen Wettbewerbsverstoß darstellt und somit einen Unterlassungsanspruch begründen kann.

Nach Inkrafttreten der DSGVO ist zwar die von vielen befürchtete Abmahnwelle bislang nicht eingetreten. Noch immer ist unklar, ob Verstöße gegen die DSGVO einen nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) abmahnfähigen Wettbewerbsverstoß darstellen. Dies wäre der Fall, wenn datenschutzrechtliche Vorschriften sogenannte „Marktverhaltensregeln“ sind. Dazu müssten die Vorschriften der DSGVO dazu bestimmt sein, im Interesse der Marktteilnehmer das Marktverhalten zu regeln. Überdies muss ein Verstoß geeignet sein, die Interessen von Mitbewerbern und Verbrauchern spürbar zu beeinträchtigen.

Bislang wurde diesbezüglich überwiegend vertreten, dass das Datenschutzrecht nicht dem Schutz von Verbrauchern als Marktteilnehmern diene, sondern vorrangig dem

Schutz des Allgemeinen Persönlichkeitsrechts. Verstöße sollten daher nicht wettbewerbsrechtlich zu ahnden sein.

Die weitere Entwicklung der Rechtsprechung bleibt abzuwarten: Das OLG Hamburg hat die Revision zugelassen, womit der BGH und der EuGH sich der Frage annehmen könnten.

Zu empfehlen ist daher, die Vorgaben der DSGVO und weiterer datenschutzrechtlicher Vorschriften – künftig auch die der e-Privacy-Verordnung – weiterhin sorgsam umzusetzen, um Abmahnungen zu vermeiden. Dazu zählt auch das Ergreifen von Maßnahmen, die dem aktuellen Stand der Technik gewährleisten (z. B. bei Kontaktformularen eine SSL- oder TLS- Verschlüsselung zu nutzen und grundsätzlich das HTTPS-Protokoll zu verwenden).

4. Anwendbarkeit des KUG

Zum Verhältnis des Kunsturheberrechtsgesetzes (KUG), das das Recht am eigenen Bild schützt, zur DSGVO hat erstmalig das OLG Köln in einem Verfügungsverfahren durch Beschluss entschieden und festgestellt, dass zumindest im journalistischen Bereich auch nach Inkrafttreten der DSGVO weiterhin das KUG gelte. Die Abwägungsmöglichkeiten des KUG seien in Einklang zu bringen sein mit unionsrechtlichen Grundrechtspositionen und entsprächen den Anforderungen der DSGVO. Nach Art. 85 Abs. 2 DSGVO sind für Datenverarbeitungen, die zu journalistischen oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgen, nationalstaatliche Ausnahmen von der Verordnung zulässig. Der Erwägungsgrund 153 führt dazu aus: „Im Recht der Mitgliedstaaten sollten die Vorschriften über die freie Meinungsäußerung und Informationsfreiheit, auch von Journalisten, Wissenschaftlern, Künstlern und/oder Schriftstellern, mit dem Recht auf Schutz der personenbezogenen Daten gemäß dieser Verordnung in Einklang gebracht werden. Für die Verarbeitung personenbezogener Daten ausschließlich zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken sollten Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung gelten, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit, wie es in Artikel 11 der Charta garantiert ist, in Einklang zu bringen. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten-

und Pressearchiven gelten. Die Mitgliedstaaten sollten daher Gesetzgebungsmaßnahmen zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Die Mitgliedstaaten sollten solche Abweichungen und Ausnahmen in Bezug auf die allgemeinen Grundsätze, die Rechte der betroffenen Person, den Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von personenbezogenen Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit und Kohärenz und besondere Datenverarbeitungssituationen erlassen. Sollten diese Abweichungen oder Ausnahmen von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein, sollte das Recht des Mitgliedstaats angewendet werden, dem der Verantwortliche unterliegt. 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." Das OLG Köln hat damit – für den journalistischen Bereich – die Fortgeltung des KUG anerkannt. Die Entscheidung erging allerdings in einem Eilverfahren. Weitere und auch höchstrichterliche Rechtsprechung dazu ist zu erwarten. Die journalistische Tätigkeit des NDR insgesamt ist geschützt durch das in § 1 NDR-Datenschutz-Staatsvertrag und § 9c RStV geregelte Medienprivileg (s. oben D. I. 2).

E. Tätigkeiten des (Rundfunk-) Datenschutzbeauftragten im Berichtszeitraum

Der Tätigkeitsschwerpunkt im Berichtsjahr 2018 lag in der Umsetzung der Datenschutzgrundverordnung, die sich auf alle Bereiche des NDR ausgewirkt hat. Darüber hinaus – und ebenfalls oft mit den Neuerungen der DSGVO verbunden – waren Vorgänge aus allen Bereichen des NDR zu bearbeiten. Grob unterteilt werden können die wesentlichen Tätigkeitsgebiete wie folgt:

- Redaktionsdatenschutz/Redaktionsgeheimnis,
- Rundfunkteilnehmerdatenverwaltung,
- Personaldatenverarbeitung,
- Organisations- und Strukturprojekte zur Verbesserung konzeptioneller und arbeitstechnischer Abläufe.

Der Verfasser des Berichts hat dazu an fast 90 Präsenzterminen im Berichtsjahr teilgenommen. Darunter waren zahlreiche Schulungen, Informations- und Austauschveranstaltungen, um in den jeweiligen Bereichen Fragen und Probleme im Umgang mit den Neure-

gelungen zu erörtern. Die folgende chronologische Auflistung der Präsenztermine in den einzelnen Bereichen bildet überblicksartig die vielfältigen Auswirkungen der DSGVO ab:

	Datum	**Angelegenheit**	**Abteilung/Ort**
1.	05.01.2018	Nutzung von Cloud-Diensten	HA Informations-, Medien- und Verbreitungstechnik (HA IMV)
2.	09.01.2018	Anpassung des Genehmigungsverfahrens im Online-Warenkorb des NDR	IT-Service Management
3.	30.01.2018	Workshop zur Umsetzung der DSGVO	Leipzig
4.	01.02.2018	Das Alte Werk/Ticketing	Programmbereich Orchester, Chor und Konzerte
5.	06.02.2018	Eignungstests für Beschäftigte im NDR	Betriebsärztin des NDR
6.	07.02.2018	DSGVO-Schulung	Service Informations- und Verbreitungssysteme (SIV)
7.	09.02.2018	Projektbegleitung	Projekte und Technologie für IT und Medien (PTIM)
8.	15.02.2018	Mitarbeiterversammlung/DSGVO-Schulung der Sendergruppe Nord	SIV, Moorfleet
9.	05.03.2018	LöschDaS Projektauftrag und Terminplanung	PTIM
10.	06.03.2018	Sitzung der Projektpartner des Virtuellen Datenschutzbüros	Hannover
11.	09.03.2018	Projektgruppe Umsetzung der DSGVO	NDR gesamt
12.	16.03.2018	Vorstellung des Berichts des NDR Datenschutzbeauftragten	Sitzung des NDR Verwaltungsrates
13.	20.03.2018	Austausch zu Neuerungen der DSGVO	Zentrale Programmaufgaben Hörfunk (ZPA HF)
14.	22.03.2018	DSGVO-konforme Kameraüberwachungen	IT-Infrastruktur (IFS)
15.	26.03.2018	Info/Austausch zum Verzeichnis von Verarbeitungstätigkeiten	ZA IMV
16.	06.04.2018	Project Active Directory (ADUBE)	PTIM

17.	06.04.2018	Projektbegleitung	PTIM
18.	13.04.2018	Projektgruppe DSGVO Umsetzung	NDR gesamt
19.	17.04.2018	Umsetzung der DSGVO	Revision
20.	19./20.04. 2018	Sitzung des AKDSB	Köln
21.	26.04.2018	Umsetzung der DSGVO	NDR Media, Studio Hamburg
22.	04.05.2018	Projekt Neubau Messwagen ZAPV	PTIM
23.	07.05.2018	Projekte E-Recruiting und Digitale Personalakte	PTIM
24.	07.05.2018	Auskunftsersuchen gemäß Art. 15 DSGVO	Abteilung Beitragsservice
25.	08.05.2018	Umsetzung der DSGVO im Landesfunkhaus Schleswig-Holstein	Kiel
26.	09.05.2018	Umsetzung der DSGVO in der PD, Technische Teilnehmerberatung und Dokumentation und Archive	HA IMV
27.	14.05.2018	Umsetzung der DSGVO	Verwaltungsdirektion
28.	14.05.2018	Umsetzung der DSGVO/Auskunftsersuchen	Intendanz
29.	15.05.2018	Projektgruppe DSGVO Umsetzung	NDR gesamt
30.	17.05.2018	Datenschutzerklärungen der Telemedienangebote des NDR	NDR gesamt
31.	23.05.2018	Umsetzung der DSGVO	Abteilung Beitragsservice
32.	24.05.2018	Umsetzung der DSGVO	Programmdirektion Hörfunk
33.	01.06.2018	Projektbegleitung	PTIM
34.	01.06.2018	Umsetzung der DSGVO	ZPA HF
35.	05.06.2018	Umsetzung der DSGVO	Markenkommunikation
36.	06.06.2018	Koordinationsgruppe IT-Sicherheit	NDR gesamt
37.	13.06.2018	Sondersitzung des AKDSB	Bonn
38.	14.06.2018	Austausch zur DSGVO - Medienprivileg	Redaktionsausschuss
39.	15.06.2018	Projektbegleitung PRODIS	PTIM
40.	19./20.06. 2018	Datenschutz-Schulungen	Hauptabteilung Personal (HA Personal)

41.	21.06.2018	Umsetzung der DSGVO/Auskunftsersuchen	Abteilung Beitragsservice
42.	22.06.2018	Gesprächskreis ARD-aktuell/ Austausch zur DSGVO - Medienprivileg	ARD-aktuell
43.	26.06.2018	Datenschutz	(N)-Team
44.	27.06.2018	Umsetzung der DSGVO	Justitiariat
45.	03.07.2018	Umsetzung der DSGVO	Einkauf und Logistik
46.	04.07.2018	Umsetzung der DSGVO	Show, Musik und Quiz
47.	06.07.2018	Nutzung der IT-Ausstattung des NDR	HA IMV
48.	11.07.2018	Project Active Directory (ADUBE)	PTIM
49.	16.07.2018	Folgen der DSGVO für die Personalien in der Betriebsöffentlichkeit, in Arbeitsverträgen	HA Personal
50.	26.07.2018	Datenschutz- und IT-Unterweisung für Personalräte	Gesamtpersonalrat
51.	31.07.2018	DSGVO Schulung Landesfunkhaus Niedersachsen	Hannover
52.	02.08.2018	Schulung der Auszubildenden	HA Personal
53.	17.08.2018	Vorstellung bei den neuen Mitglieder des NDR Verwaltungsrats	Verwaltungsrat des NDR
54.	20.08.2018	Eignungsuntersuchungen im Arbeitsvertrag	HA Personal
55.	21.08.2018	Umsetzung der DSGVO Betriebssport	Betriebssport des NDR
56.	22.08.2018	Teilnahme an der Abteilungssitzung, Fragen/Austausch zur DSGVO	IFS
57.	24.08.2018	Datenschutzerklärung der Telemedienangebote des NDR	PB Online und Multimedia
58.	28.08.2018	AG Multimedia	Gesamtpersonalrat
59.	06.09.2018	Teilnahme an der Sitzung des Rechts- und Eingabenausschusses	Rechts- und Eingabenausschuss des NDR Rundfunkrats
60.	07.09.2018	Umsetzung der DSGVO	Personalrat Hamburg
61.	07.09.2018	DSGVO Schulung der Auszubildenden	HA Personal
62.	13.09.2018	Projektgruppe Umsetzung der DSGVO	NDR gesamt
63.	14.09.2018	Besucherausweise	Studioküche
64.	18.09.2018	Teilnahme an der Sitzung der AG Telemedien	AG Telemedien des Programmausschusses

			des NDR Rundfunkrats
65.	21.09.2018	Projektbegleitung	PTIM
66.	25.09.2018	Einsatz von Umfragetools	Programmdirektion Fernsehen
67.	26.09.2018	Dienstanweisungen Datenschutz	HA IMV
68.	27.09.2018	DSGVO Schulung	Systemservice – Landesfunkhaus Schleswig-Holstein
69.	28.09.2018	Opt-in bei Datenjournalismus-Projekt	ARD-aktuell
70.	08.10.2018	Besuch von Beschäftigten von Facebook	NDR gesamt
71.	18.10.2018	Audit bei einem Auftragsverarbeiter	Köln
72.	22.10.2018	Projektbegleitgruppe AG News	Crossmediales Nachrichtenhaus
73.	22.10.2018	Fragen/Austausch/DSGVO Schulung	Zentrale Aufgaben PD
74.	24.10.2018	Fragen/Austausch zur DSGVO	Außenübertragung FS
75.	25.10.2018	Dienstanweisungen Datenschutz	Produktionsdirektion
76.	29.10.2018	Einblicke gewinnen, Netzwerk aufbauen, Wissen teilen	HA Personal
77.	07.-09.11.2018	Sitzung des AKDSB	Mainz
78.	12.11.2018	Schulung der neuen Volontäre	HA Personal
79.	12.11.2018	Projektbegleitgruppe Newsroom ARD-aktuell	ARD-aktuell
80.	13.11.2018	Koordinationsgruppe IT-Sicherheit	NDR gesamt
81.	15.11.2018	Beratungstermin Arbeitssicherheit/DS	Arbeitssicherheit
82.	16.11.2018	Projektbegleitung	PTIM
83.	27.11.2018	Lenkungsaustausch Neue Techniken	NDR gesamt
84.	27.11.2018	EDV- und Technikforum	NDR gesamt
85.	28. /29.11. 2018	Umsetzung der DSGVO	ZBS, Köln
86.	30.11.2018	Dienstvereinbarung digitale Telekommunikationssysteme	IFS
87.	04.12.2018	Dienstanweisungen Datenschutz	Produktionsdirektion
88.	06.12.2018	Personalversammlung	Oldenburg
89.	07.12.2018	PRODIS Projektbegleitung	PTIM

Diese Aufstellung bildet nur die jeweils vor Ort wahrgenommen Termine ab. Aus diesen wird deutlich, wie weitreichend sich datenschutzrechtliche Belange in allen Bereichen des NDR auswirken. Im Folgenden werden die Tätigkeiten im Berichtsjahr systematisch zugeordnet und erschöpfend dargestellt.

I. Umsetzung der DSGVO

Im Dezember 2017 wurde eine Projektgruppe zur Umsetzung der Datenschutzgrundverordnung im NDR eingesetzt, in denen Vertreter*innen aus allen Direktionen mitgewirkt haben. Bis zum 25. Mai 2018 wurde eine Bestandsaufnahme bezüglich der Verarbeitungstätigkeiten von personenbezogenen Daten im NDR durchgeführt und die wesentlichen Anpassungsmaßnahmen vorgenommen. Diese betrafen insbesondere:

1. Anpassungen der Datenschutzerklärungen

Sämtliche Datenschutzerklärungen der vom NDR verantworteten (Telemedien-) Angebote mussten angepasst werden. Dies betraf u. a. ndr.de, tagesschau.de, das Intranet des NDR und weitere spezifische Ausspielformen (z. B. die ARD Quizz App, die Tagesschau-App, HbbTV-Angebote). Die Erklärungen sind dadurch deutlich länger, aber auch transparenter geworden und geben zum Beispiel Hinweise zu Dienstleistern, Messmethoden bezüglich der Onlinenutzung und detaillierte Informationen zu Drittanbietern an. Auch wurden Hinweise zur Wahrnehmung von Rechten gemäß Art. 15 ff. DSGVO aufgenommen.

In möglichst einfacher Sprache werden Nutzer*innen u. a. über die Erhebung personenbezogener Daten bei Online-Serviceangeboten informiert und der Einsatz von Cookies erläutert. Um dem Gebot der Datensparsamkeit zu entsprechen, besteht die Möglichkeit, der Anzeige von eingebetteten Inhalten von Drittanbietern wie Facebook, YouTube, Twitter und Instagram selbst zuzustimmen.

Die Datenschutzerklärungen sind stets aktuell zu halten und an die fortwährenden Einwicklungen (z. B an den Einsatz anderer Drittanbieter) anzupassen. Zu erwähnen ist an dieser Stelle auch, dass die Bereitstellung eines Telemedienangebots technisch komplex und vielschichtig ist, was sich in der schriftlichen Darstellung sämtlicher Anwendungen und Funktionen in den Datenschutzerklärungen niederschlägt. Erfreulich ist daher, dass einige Nutzer*innen konstruktive Hinweise gegeben oder Fra-

gen gestellt und somit zur Abrundung der Erklärungen einen wertvollen Beitrag geleistet haben.

Pünktlich zum Inkrafttreten der Datenschutzgrundverordnung am 25. Mai 2018 wurden die neuen Erklärungen veröffentlicht. Zu finden sind sie z. B. unter https://www.ndr.de/service/datenschutz/index.html und https://www.tagesschau.de/kontakt_und_hilfe/datenschutz/index.html.

2. Veröffentlichung der proaktiven Informationen nach Art. 13 DSGVO

Art. 13 DSGVO sieht umfangreiche Informationen vor, die bereitgestellt werden müssen, wenn personenbezogene Daten bei einer Person erhoben werden. Zum Zeitpunkt der Erhebung der Daten sind u.a. folgende Angaben mitzuteilen:

- der Namen und die Kontaktdaten des Verantwortlichen (NDR) sowie gegebenenfalls seines Vertreters,
- die Kontaktdaten des Datenschutzbeauftragten,
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen,
- die Rechtsgrundlagen für die Verarbeitung,
- gegebenenfalls berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden,
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln,
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder 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 Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit,
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte.

Zwecks Umsetzung dieser Transparenzverpflichtung wird insbesondere im Anschluss an die Datenschutzerklärungen für alle Möglichkeiten einer Datenverarbeitung über diese Punkte informiert. Die praktische Umsetzung dieser Vorgaben ist wie folgt vorgenommen worden:

„11. Weitere Information gem. Art. 13 Datenschutzgrundverordnung
11.1 Grundsätze der Verarbeitung personenbezogener Daten
Weiterhin informieren wir Sie hiermit – unabhängig von der Nutzung unserer Onlineangebote – über den Umgang mit Daten im NDR: Im Zeitpunkt der Datenerhebung, beispielsweise im Rahmen einer Vertragsbeziehung zur Erfüllung gegenseitig geschuldeter Leistungen und Pflichten oder in Wahrnehmung des Hausrechts und ggf. damit einhergehenden berechtigten Sicherheitsinteressen speichert der NDR personenbezogene Daten von Ihnen. Dies können beispielsweise sein:
Name, Kontaktdaten, Geburtsdatum, Bankverbindung, Arbeitgeber, Auftraggeber, Personalausweis- oder Führerscheindaten, haussicherheitsrelevante Daten wie Personenbilder aus videoüberwachten Zutrittsbereichen und andere Zutrittsdaten, Logdateien und IP-Adressen, Bilder oder Filmaufnahmen bei Konzerten oder sonstigen Veranstaltungen des NDR.

Personenbezogene Daten werden zu jeweils ganz unterschiedlichen Zwecken und immer auf gesetzmäßiger Grundlage verarbeitet, beispielsweise:

Vertragsanbahnung und -erfüllung (Art. 6 Abs. 1 b) DSGVO), z. B. um Ihnen

- Zutritt zu unserem Grundstück und Räumlichkeiten im Rahmen von Auftragsbeziehungen oder bei Veranstaltungen oder auch zur Kantinennutzung gewähren zu können,
- eine von Ihnen angefragte Leistung zur Verfügung stellen zu können (bspw. Newsletter, Programmheft, personalisierter Zugang zu bestimmten Internetangeboten),
- eine Gewinnspiel- oder Verlosungsteilnahme zu ermöglichen,

Schutz lebenswichtiger Interessen eines Betroffenen (Art. 6 Abs. 1 d) DSGVO),

- beispielweise Einsichtnahme in und Weitergabe von personenbezogenen Daten im Falle eines Unfalles, falls der Betroffene selbst nicht auskunftsfähig sein sollte;

Wahrnehmung des Rundfunk- und Programmauftrags des NDR als Aufgabe, die im öffentlichen Interesse liegt (Art. 6 Abs. 1 e) DSGVO),

- beispielsweise Bearbeitung von Hörerpost oder Programmbeschwerden;

Wahrung berechtigter Interessen des NDR in Abwägung mit den Grundrechten und Grundfreiheiten der Betroffenen (Art. 6 Abs. 1 f) DSGVO),

- beispielsweise Verarbeitung von personenbezogenen Daten für die Außendarstellung des NDR oder in Wahrnehmung des Hausrechts (insbesondere Sicherheitsinteressen).

11.2 Verpflichtung zur Bereitstellung und Konsequenzen der Nichtbereitstellung
Die Bereitstellung solcher personenbezogener Daten ist zur Erreichung der genannten Zwecke erforderlich und ggf. ein wesentlicher Teil Ihrer vertraglichen Pflichten gegenüber dem NDR. Das Nichtbereitstellen der personenbezogenen Daten kann zur Folge haben, dass Ihnen eine vertragliche Leistung nicht zur Verfügung gestellt werden kann, die Vertragsbeziehung beendet werden muss, oder Ihnen ggf. kein Zugang zum Grundstück oder den Räumlichkeiten des NDR gewährt werden kann, bzw. Sie diese bei Aufforderung umgehend verlassen müssen.

11.3 Datenverarbeitungen aufgrund von Einwilligung und Widerrufsrecht, Art. 6 Abs. 1 a) DSGVO
Sollte der NDR zusätzlich auf Grundlage freiwilliger Einwilligung (Art. 6 Abs. 1 a), Art. 4 Nr. 11 DSGVO) personenbezogene Daten von Ihnen erhalten und verarbeiten, haben Sie jederzeit das Recht, eine solche Einwilligung ohne Angabe von Gründen für die Zukunft zu widerrufen. Die Rechtmäßigkeit der bis zum Widerruf der Einwilligung erfolgten Verarbeitungen bleibt davon unberührt. [...]

11.4 Empfänger der Daten beim NDR und Datenweitergabe an Dritte
Empfänger Ihrer personenbezogenen Daten sind die jeweils mit konkreten zweckgebundenen Aufgaben beim NDR betrauten Personen (beispielsweise Abteilungs- und Redaktionsmitarbeiter, Empfangs-, Sicherheits-, Veranstaltungs- oder Kantinenpersonal). Diese sind verpflichtet, die Vertraulichkeit Ihrer Daten gemäß den Vorgaben der DSGVO zu wahren. Darüber hinaus geben wir Ihre personenbezogenen Daten nicht an Dritte weiter, es sei denn, Sie haben in die Datenweitergabe eingewilligt oder wir sind aufgrund gesetzlicher Bestimmungen und/oder behördlicher oder gerichtlicher Anordnungen zu einer Datenweitergabe verpflichtet.

11.5 Auftragsdatenverarbeitung und Datensicherheit

Aufgrund gesonderter schriftlicher Vereinbarungen lassen wir personenbezogene Daten auch von Dienstleistern im Rahmen von Auftragsverarbeitungsverhältnissen gem. Art. 28 DSGVO verarbeiten. Hiermit sind keine Übermittlungen Ihrer persönlichen Daten an Dritte im datenschutzrechtlichen Sinne verbunden. Der NDR bleibt Ihnen gegenüber datenschutzrechtlich verantwortlich.

Die Mitarbeiterinnen und Mitarbeiter der Auftragsverarbeiter sind zur Wahrung der Vertraulichkeit Ihrer Daten verpflichtet wie unsere eigenen Beschäftigten. Sie unterliegen unseren Weisungen. Alle gesetzlich vorgeschriebenen technischen und organisatorischen Sicherheitsmaßnahmen zum Schutz Ihrer personenbezogenen Daten vor Verlust und Missbrauch werden vom NDR gewährleistet. So werden Ihre personenbezogenen Daten jeweils in sicheren Betriebsumgebungen gespeichert, die Mitarbeitern der Auftragsverarbeiter nur insoweit zugänglich sind, als dies zur Erfüllung der vertraglichen Aufgaben zwingend erforderlich ist.

11.6 Kriterien für die Festlegung von Speicherdauern

Ihre personenbezogenen Daten werden beim NDR solange gespeichert, bis die Vertragsbeziehung endgültig beendet ist, sich keine weiteren gegenseitigen Ansprüche mehr daraus ergeben können und auch die gesetzlichen oder internen Aufbewahrungsfristen des NDR abgelaufen sind.

Personenbezogene Daten, die wir in Wahrnehmung unserer Aufgaben im öffentlichen Interesse oder aufgrund von berechtigten Unternehmensinteressen verarbeiten, werden solange gespeichert, bis der Zweck erfüllt bzw. die Aufgabe erledigt ist und eine Dokumentation, insbesondere auch zu etwaigen Beweiszwecken zur Rechtewahrung oder Rechtsverfolgung, nicht mehr erforderlich ist.

11.7 Ihre Auskunfts- und Beschwerderechte

Sie haben das Recht, vom NDR Auskunft über die Sie betreffenden personenbezogenen Daten zu verlangen sowie ggf. Berichtigung, Löschung und Einschränkung der Verarbeitung oder ggf. auch das Recht, einen Widerspruch geltend zu machen (Betroffenenrechte gem. Art. 15 ff. DSGVO). Unter den Voraussetzungen von Art. 20 DSGVO kann ein Recht auf Datenübertragung in Betracht kommen. Schließlich haben Sie das Recht, sich bei der Aufsichtsbehörde zu beschweren, wenn Ihrer Ansicht nach ein Verstoß gegen das Datenschutzrecht vorliegt. […]“

Überall dort, wo der NDR Kontaktadressen veröffentlicht oder Service anbietet, wird nunmehr auf diese Informationen und die Datenschutzerklärungen verwiesen.

Die Ausführungen sind ausführlich und erschöpfend und entsprechen damit der umfangreichen gesetzlichen Verpflichtung. Auch diesbezüglich bedarf es einer kontinuierlichen Aktualisierung der Informationen.

3. Gewinnspiele, Hinweise bei Sprachassistenten und Nutzungen von Drittplattformen

Überarbeitungsbedürftig waren auch die Erklärungen zu Gewinnspielen, um hinreichende Transparenz bezüglich der Speicherung von Daten von Teilnehmer*innen und Gewinner*innen zu gewährleisten.

Darüber hinaus wurden, ohne dass dies rechtlich zwingend erforderlich wäre, Hinweise und Erläuterungen aufgenommen, wenn auf Inhalte des NDR außerhalb der eigenen Angebote verwiesen wird (z. B. wie folgt: „Dienste wie Facebook haben leider andere Datenschutz-Standards als der NDR. Der NDR hat auf die datenschutzrechtlichen Bestimmungen und Einstellungen dieser Plattformen keinen Einfluss. Im Rahmen unserer Möglichkeiten gehen wir jedoch mit der größten Sensibilität mit Ihren Daten um.“) Zudem wird auf Plattformen Dritter, wie etwa bei Facebook, immer auch auf die vom NDR verantworteten Telemedienangebote hingewiesen:

„Besuchen Sie uns auch auf NDR.de oder in unseren kostenfreien NDR Apps. Dort erwarten Sie regionale und nationale Nachrichten, Informationen, Unterhaltung und vieles mehr.
Datenschutz
Der NDR hat auf die datenschutzrechtlichen Bestimmungen dieser Plattform sowie die Erhebung, Analyse und Nutzung von Userdaten keinen Einfluss. In seinen Datenrichtlinien erklärt Facebook, welche Daten bei der Nutzung erhoben werden. […]: Jeder Facebook-Nutzer hat die Möglichkeit, eine Kopie seiner aufgezeichneten Daten zu beantragen […] Wir raten dazu, die vielfältigen Datenschutz- und Sicherheitseinstellungen zu nutzen und regelmäßig zu überprüfen. Eine Anleitung finden Sie hier: […] Im Rahmen unserer Möglichkeiten gehen wir mit der größten Sensibilität mit Ihren Daten um. Weitere Informationen zum Thema Datenschutz finden Sie auf unserer Website: www.ndr.de/service/datenschutz“.

Durch derartige Hinweise soll ein Beitrag zur Sensibilisierung der Nutzer*innen für datenschutzrechtliche Belange geleistet werden.

4. Organisation eines Verfahrens zur Beauskunftung von Anfragen gemäß Art. 15 DSGVO

Das in Art. 15 DSGVO niedergelegte Auskunftsrecht von Personen, deren personenbezogene Daten von einem Verantwortlichen verarbeitet werden, ist weit gefasst. Die Erwägung des Gesetzgeber dazu lautet: „Jede betroffene Person sollte […] ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht."

Der NDR tritt in vielfältiger Weise in Kontakt mit Personen und verarbeitet dabei auch personenbezogene Daten. Dies ist etwa der Fall

- bei Gewinnspielen oder Verlosungen,
- beim Abonnement von Newslettern,
- beim Einzug der Rundfunkbeiträge,
- bei der technischen Teilnehmerberatung

und in vielen anderen Konstellationen. Um die jeweiligen Zwecke zu erfüllen, bedarf es entsprechender Daten. Um über diese Auskunft zu geben, müssen daher alle Bereiche des NDR – dieser ist Adressat des Anspruchs – mitwirken und ermitteln, ob und ggf. welche Daten über eine anfragende Person verarbeitet werden. Das dazu entwickelte Verfahren wird in der Intendanz von der Markenkommunikation gesteuert, indem dort alle eingehenden Auskunftsanfragen gebündelt, in die Direktionen des NDR verteilt und die Rückmeldungen zusammengefasst werden.

Weitere Ausführungen zur Wahrnehmung des Auskunftsanspruches und Bearbeitung der Anfragen sind den folgenden Ausführungen unter III. – Teilnehmerdatenverwaltung zu entnehmen. Denn es hat sich gezeigt, dass der Schwerpunkt der Auskunftsersuchen beim Rundfunkbeitragseinzug liegt. Auskünfte und Beschwerden stehen

ganz wesentlich im Zusammenhang damit. Dies bindet Kapazitäten, zumal die Anfragen umfangreicher und auch inhaltlich komplexer werden. Zu verzeichnen ist zudem ein Anstieg von Anfragen, die wiederholt gleichlautende Anträge stellen und/oder den hoheitlichen Charakter des Beitragseinzugs nicht akzeptieren wollen.

5. Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)

„Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können“ (Erwägungsgrund 82 DSGVO)“.

Die weit gefasste Anforderung des DSGVO wurde für den NDR so organisiert, dass das Verzeichnis der Verarbeitungstätigkeiten dezentral von allen Bereichen des NDR bestückt wird. Überall dort, wo im NDR Datenverarbeitungstätigkeiten durchgeführt werden, muss der dafür zuständige Bereich ein vom AKDSB abgestimmtes Musterblatt ausfüllen und im zentralen Verzeichnis des NDR elektronisch ablegen. Zugleich ist sicherzustellen, dass das Verzeichnis laufend aktualisiert und ergänzt wird.

6. Etablierung eines Verfahrens zur Datenschutzfolgeabschätzung nach Art. 35 DSGVO

Die Datenschutzfolgeabschätzung ist ein neues Instrument der DSGVO. Die gesetzliche Vorgabe lautet: „Hat eine Form der Verarbeitung, 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.“

Das bedeutet, dass der Verantwortliche (NDR) vor der Verarbeitung personenbezogener Daten eine Datenschutzfolgenabschätzung durchführen muss, mit der die spezi-

fische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.

Dieses Verfahren ähnelt einer sogenannten Schutzbedarfsfeststellung, bei der in Datenverarbeitungsprozessen ermittelt wird, welche Risiken für die IT-Sicherheit des NDR bestehen können. Die Schutzbedarfsfeststellung ermittelt mithin IT- Risiken für den NDR, die Datenschutzfolgenabschätzung dient der Ermittlung von Risiken für etwaig betroffene Personen. Aufgrund der „Verwandtheit" beider Verfahren wurden diese in einem Prozess zusammengeführt. Die entsprechende Anforderung der DSGVO ist damit umgesetzt.

7. Kameraüberwachungen

Die DSGVO enthält keine speziellen Ausführungen zu den Voraussetzungen von Kameraüberwachungen Für Kameraüberwachungen gelten die allgemeinen Vorschriften zur Datenverarbeitung, die durch § 4 BDSG-neu, der im Wesentlichen die Regelung des bisherigen § 6b BDSG-alt wiedergibt, noch weiter konkretisiert wurden. Auch der NDR muss also die sich daraus ergebenden Vorgaben erfüllen, um rechtmäßig Kameraüberwachungen durchzuführen. Die wesentlichen Maßstäbe sind:

- Gemäß Art. 6 Abs. 1 e), f) DSGVO in Verbindung mit § 4 Abs. 1 BDSG, muss der verantwortliche Betreiber derartiger Kameras einen privilegierten Zweck mit der Überwachung zu verfolgen. Ein solcher kann z. B. bei der Aufgabenerfüllung öffentlicher Stellen vorliegen, bei der Wahrnehmung des Hausrechts oder bei der Wahrnehmung berechtigter Interessen für weiter konkret festgelegte Zwecke.
- Das Merkmal des Hausrechts umfasst insbesondere den Schutz des eigenen Objektes, also etwa auch des Betriebsgeländes.
- Das Merkmal der berechtigten Interessen spielt eine überragende Rolle. Dabei müssen nicht nur legitime eigene Interessen vorhanden sein, sondern das schutzwürdige Interesse der Beobachteten darf zudem nicht überwiegen.
- Die Feststellung, was zu den legitimen Interessen des Verantwortlichen Betreibers gehört und welches Gewicht dieses im Gegensatz zum Recht auf Nicht-

Beobachtung der von der Kamera erfassten Personen hat, ist von maßgeblicher datenschutzrechtlicher Bedeutung. Zu beachten sind auch die Interessen Dritter.

- Die Rechtsgüter Leben, Freiheit und Gesundheit sind im Rahmen des Einsatzes bei einer Interessenabwägung stets zu beachten. Das berechtigte Interesse des Betreibers alleine reicht nicht aus. Die Überwachungsanlage muss zudem auch geeignet sowie das mildeste Mittel sein, den konkreten Zweck zu erreichen.
- Wenn die geplante Videoüberwachung diesen Anforderungen gerecht wird, treffen den Verantwortlichen jedoch noch weitere Pflichten (Transparenz, Hinweis auf Betroffenenrechte).
- Zudem muss die etwaige Speicherung von Aufnahmen auf das notwendige Maß begrenzt sein und auf den Umstand der Überwachung muss frühestmöglich hingewiesen werden.

Die Kameraüberwachungen der Gelände des NDR wurde an diesen Grundsätzen überprüft und entsprechend ausgewiesen. Neben den Symbolen an den überwachten Bereichen wurden zudem weitere Erläuterungen zum Grund, zu den Rechtsgrundlagen und Rechten von Betroffenen erstellt, ausgelegt bzw. im Internet bei den „Wegweisern zum NDR“ (https://www.ndr.de/der_ndr/standorte_und_adressen/Wegweiser-zum-Norddeutschen-Rundfunk,wegweiser6.html) veröffentlicht. Das dort abrufbare „Informationsblatt zur Videoüberwachung im NDR“ enthält alle relevanten und geforderten Informationen zu dieser Thematik.

8. Auftragsverarbeitungen

Art. 28 DSGVO regelt die sog. Auftragsverarbeitung. Dort heißt es in Absatz 1: „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“

Der Gesetzgeber hat dazu folgende Erwägungen aufgestellt: „Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verar-

beitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind."

In der Praxis gibt es eine Vielzahl von Auftragsverarbeitungen für den NDR. Der Überarbeitungsbedarf war daher enorm. Um die Belastungen abzufedern, haben die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio ein Musterformular entworfen, um den erheblichen Arbeitsaufwand durch Standardisierungen zu begrenzen. Gleichwohl kommt es nicht selten zu langwierigen und zähen Auseinandersetzungen über einzelne Vertragsklauseln, die von den entsprechenden Fachabteilungen auszuhandeln und zu vereinbaren sind. Der Rundfunkdatenschutzbeauftragte steht auch diesbezüglich beratend zur Seite, kann aber maßgeblich als Aufsichts- und Kontrollorgan des NDR nicht das operative Geschäft führen.

9. Anpassung sonstiger Verträge und Muster

Neben dem Muster zur Auftragsverarbeitung waren weitere Muster und Handlungsanweisungen zu erstellen, um die Umsetzung der Datenschutzgrundverordnung sicherzustellen. Im Zusammenarbeit mit den Datenschutzbeauftragten der anderen Landesrundfunkanstalten, der Deutschen Welle, des ZDF und Deutschlandradio wurden sogenannte Fact Sheets erstellt, die einzelne Themenkomplexe erläutern und Handlungsempfehlungen geben. Es wurde etwa ein Mustervertrag zum Joint Controllership gemäß Art. 26 DSGVO entwickelt, die „Zusätzlichen Vertragsbedingungen des Norddeutschen Rundfunks für die Vergabe von Dienst- und Lieferaufträgen von Produktionsvertragen" sowie Einkaufsbedingungen angepasst und weitere Standardverträge ergänzt.

II. Redaktionsdatenschutz/Redaktionsgeheimnis

§ 1 Abs. 1 S. 1 bis 3 NDR-Datenschutz-Staatsvertrag lautet: „Soweit der NDR personenbezogene Daten zu journalistischen Zwecken verarbeitet, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort."

Mit der Aufnahme eines Beschäftigungsverhältnisses beim NDR wurden bereits vor Geltung des NDR-Datenschutz-Staatsvertrags alle Personen, unabhängig von ihrem Beschäftigungsstatus, auf das Datengeheimnis verpflichtet. Auf Anregung des Verfassers dieses Berichts wurde dies für alle Beschäftigten, unabhängig von der im NDR ausgeübten Tätigkeit, wiederholt.

Auch wenn die datenschutzrechtlichen Neuregelungen seit dem 25. Mai 2018 eine solche Verpflichtung nicht explizit für alle Beschäftigten vorschreiben, ergibt sich zum einen aus Art. 5 DSGVO, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Überdies obliegt dem Verantwortlichen NDR die Pflicht, die Einhaltung dieser Vorgabe nachweisen zu können („Rechenschaftspflicht"). Diese Pflicht kann durch eine dokumentierte Verpflichtungserklärung erfüllt werden. Die Notwendigkeit einer Verpflichtungserklärung ergibt sich weiterhin aus Art. 24 DSGVO. Dort geht es um das Erfordernis technischer und organisatorischer Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO – und damit auch entsprechend den Grundsätzen des Art. 5 DSGVO – erfolgt. Weitere Anknüpfungspunkte für eine Verpflichtung auf das Datengeheimnis ergeben sich aus Art. 29 und 32 DSGVO.

Die Personalabteilung des NDR hat daher mit einem entsprechenden, zur Verfügung gestellten Muster für eine Verpflichtungserklärung auf das Datengeheimnis, das für alle Arten von Beschäftigungsverhältnissen geeignet ist (feste/freie Mitarbeiter*innen, Auszubildende, Praktikant*innen, Volontär*innen, ...), diese Verpflichtungen eingeholt. Begleitet wurde diese Maßnahme durch Veröffentlichungen im Intranet.

Nicht nur die Umsetzung der Verpflichtung aus § 1 Abs. 1 NDR-Datenschutz-Staatsvertrag, auch die weiteren Neuerungen im Datenschutzrecht haben zu regen Nachfragen, Informationsveranstaltungen und Austauschen mit den Redaktionen geführt. Im Kern ging es um das Medienprivileg: Erörtert wurden insbesondere die Bedeutung und Reichweite des Medienprivilegs, die Auswirkungen im redaktionellen Alltag, etwaige Neuerungen hinsichtlich der Einholung von Einwilligungserklärungen sowie das Anfertigen von Bild- und Tonmaterial für redaktionelle Zwecke.

Außerdem haben den Rundfunkdatenschutzbeauftragten zu einzelnen Sendungen des NDR Zuschriften von Bürger*innen erreicht, mit denen durch die Ausstrahlung der Bei-

träge Verletzungen des Rechts auf informationelle Selbstbestimmung geltend gemacht wurden. Beanstandet wurde zumeist, dass keine Einwilligungen erteilt oder diese widerrufen worden seien. Die geltend gemachten Ansprüche bestanden in aller Regel nicht, in einigen Fällen konnte durch die Bearbeitung der Beiträge Abhilfe geschaffen werden.

Auch die Redaktionen haben in vielfältiger Weise Beratungen erbeten, etwa zu Fragen zu den Bedingungen von Akkreditierungen für die Spiele der Bundesliga, im Zusammenhang mit der Erhebung von Daten bei interaktiven Angeboten im Rahmen der ARD-Themenwoche und des Eurovision Song Contests, beim Umgang von Datenbanken mit Expert*innen-Kontakten, Online-Umfragetools und sonstigen On- und Off-Air-Veranstaltungen.

III. Rundfunkteilnehmerdatenverwaltung

Obgleich es schon vor Geltung der DSGVO die Möglichkeit für Betroffene gab, Auskünfte über die Verarbeitung von personenbezogenen Daten einzuholen, wurde das neu durch Art. 15 DSGVO ausgeformte Recht – auch durch entsprechende Berichterstattungen in den Medien und Aufrufen zur Einholung derartiger Auskünfte in sozialen Medien – häufig in Anspruch genommen. In vielen Fällen wurde durch im Internet abrufbare standardisierte Schreiben von diesem Recht Gebrauch gemacht.

Insgesamt sind im Berichtsjahr bis zum 25. Mai 2018 sieben Auskunftsersuchen beim (Rundfunk-) Datenschutzbeauftragten eingegangen, die alle beauskunftet werden konnten. Seit Geltung der DSGVO am 25. Mai 2018 haben den NDR weitere 98 Auskunftsersuchen erreicht. Im Jahr 2018 konnten 88 dieser weiteren Ersuchen beantwortet werden. 5 Anfragen wurden mangels hinreichender Identifizierung der Anfragenden nicht beantwortet, da die Gefahr bestand, dass eine Übermittlung personenbezogener Daten an nicht berechtigte Personen erfolgt. Erwägungsgrund 64 der DSGVO sieht vor, dass der Verantwortliche alle vertretbaren Mittel nutzen soll, „um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen“. Erbeten wurden daher die Einreichung eines unterzeichneten Auskunftsersuchens und/oder die Mitteilung der neunstelligen Beitragsnummer, um dieser Anforderung gerecht zu werden. Diese erbetenen Angaben wurden in den genannten 5 Fällen nicht nachgereicht. Überdies wurden, teilweise im Zusammenhang mit einem Auskunftsersuchen oder aufgrund anderer Zuschriften, 27 Begehren an den Rundfunkdatenschutzbeauftragten gerichtet, die sich auf die Daten-

verarbeitung zum Zwecke des Beitragseinzugs bezogen. Dabei ging es um Datenübermittlungen aufgrund des Meldedatenabgleichs gemäß § 14 Abs. 9a RBStV, Fragen zum Grund und der Datenverarbeitung insgesamt und zu einzelnen personenbezogenen Daten (z. B. der Lage einer Wohnung, Doktortitel), Geltendmachungen von Datenschutzverletzungen sowie Ansprüche auf Löschung und Widerruf. Die daraufhin erfolgte Prüfung hat jeweils keine Verletzung datenschutzrechtlicher Vorgaben ergeben.

Insgesamt hat sich die Anzahl der Eingaben und Auskunftsersuchen gegenüber dem Vorjahr (2017: 22) deutlich erhöht. Dies gilt auch für die entsprechenden Vorgänge beim Beitragsservice von ARD, ZDF und Deutschlandradio in Köln (ZBS), wie die folgenden Tabellen zeigen:

Datenschutzrechtliche Eingaben **bis zum 24.05.2018** beim ZBS											
Vorgangsart	BR	HR	MDR	**NDR**	RBB	RB	SR	SWR	WDR	Unb.	Gesamt
Ersuchen von Bürgern um Auskunft über zu ihrer Person gespeicherte Daten	57	29	38	**55**	48	3	6	64	67	-	**367**
Fragen bezüglich der Herkunft von Daten (z.B. Adressen) bzw. der Berechtigung zur Datenerhebung	3	2	5	**3**	4	-	-	3	2	-	**22**
Verlangen, gespeicherte personenbezogene Daten zu löschen, zu sperren oder zu berichtigen	11	3	8	**8**	8	1	-	9	11	-	**59**
Verlangen, Beitragszahlerdaten nicht zu anderen Zwecken zu nutzen bzw. zu übermitteln	-	-	-	**-**	-	-	-	-	-	-	**-**
Andere, nicht den vorstehenden Fallgruppen zuzuordnende Anfragen bzw. Eingaben zum Datenschutz	5	3	3	**5**	2	-	-	-	1	3	**22**
Anfragen von Finanzämtern nach Daten (insbes. Bankverbindungen) von Beitragszahlern	-	-	3	**2**	-	-	-	-	2	-	**7**
Anfragen von Kommunalkassen oder sonstigen Stellen nach Daten (Adressen, Bankverbindungen) von Beitragszahlern	2	-	1	**3**	8	-	-	2	4	-	**20**
Anzahl Vorgänge insgesamt (bis 24.05.18)	**78**	**37**	**58**	**76**	**70**	**4**	**6**	**78**	**87**	**3**	**497**

Datenschutzrechtliche Eingaben **ab dem 25.05.2018** beim ZBS											
Vorgang	BR	HR	MDR	**NDR**	RB	RBB	SR	SWR	WDR	Unb.	Gesamt
Auskünfte gem. Art. 15 DSGVO	1121	454	578	**946**	55	567	54	1063	1157	-	5995
Sonst. Schreiben (Fragen zur Datenherkunft, Löschungsverlangen, weitere Ansprüche)	21	12	15	**18**	1	14	3	20	29	7	**140**
Gesamtsumme Vorgänge (ab 25.05.18)	**1142**	**466**	**593**	**964**	**56**	**581**	**57**	**1083**	**1186**	**7**	**6135**

Hinsichtlich der Rundfunkteilnehmerdatenverwaltung hat überdies die Umsetzung des Urteils des Bundesverfassungsgerichts zur Verfassungsmäßigkeit des Rundfunkbeitrags mit Blick auf Nebenwohnungen datenschutzrechtliche Probleme und Anfragen ausgelöst. Mit Urteil vom 18. Juli 2018 hatte das Gericht entschieden, dass die Rundfunkbeitragspflicht im privaten Bereich an das Innehaben von Wohnungen anknüpfen darf, weil Rundfunkangebote typischer Weise dort genutzt werden. Inhaber mehrerer Wohnungen dürften für die Möglichkeit privater Rundfunknutzung allerdings nicht mit insgesamt mehr als einem vollen Rundfunkbeitrag belastet werden. Eine Rundfunkbeitragspflicht für Nebenwohnungen besteht mithin grundsätzlich nicht. Die Umsetzung dieses Urteils beim Zentralen Beitragsservice berührte insofern datenschutzrechtliche Fragen, als zu klären war, welche Angaben auf einem entsprechenden Antragsformular für eine Freistellung von der Beitragspflicht verlangt werden können.

Bezüglich des sog. erneuten Meldedatenabgleichs beim Rundfunkbeitragseinzug gemäß § 14 Abs. 9a Rundfunkbeitragsstaatsvertrag waren die Anzahl der Fragen und Beschwerden insgesamt gering. Der Abgleich des Teilnehmerbestandes beim Beitragsservice mit den Daten der volljährigen Einwohner bei den Einwohnermeldeämtern verfolgt das Ziel der Überprüfung der Richtigkeit des Datenbestandes und der Gewährleistung der Beitragsgerechtigkeit. Der Abgleich der Datensätze löste insbesondere Fragen zur Rechtsgrundlage der Datenübermittlung und deren Wirksamkeit aus. Die Prüfungen des Rundfunkdatenschutzbeauftragten kamen in allen Fällen zu dem Ergebnis, dass datenschutzrechtliche Vorschriften nicht verletzt wurden.

Gegenstand regelmäßiger Prüfungen sind zudem die Löschkonzepte des Beitragsservice, die maßgeblich die Anforderung der Speicherbegrenzung (Art. 5 Abs. 1 lit e) DSGVO zum Ziel haben. Danach müssen personenbezogenen Daten „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung")". Die Grundsätze der Löschung von personenbezogenen Daten, die zum Zwecke des Rundfunkbeitragseinzugs verarbeitet werden, entsprechen den gesetzlichen Anforderungen und lauten wie folgt:

„Die erhobenen Daten werden vom Beitragsservice unverzüglich gelöscht, wenn feststeht, dass sie für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden, die betroffene Person ihre Einwilligung, auf die eine Verarbeitung gestützt wurde, widerruft oder personenbezogene Daten unrechtmäßig verarbeitet wurden. Eine Löschung der entsprechenden Daten erfolgt beispielsweise, wenn keine Beitragspflicht mehr besteht, oder aufgrund des Widerrufs eines erteilten SEPA-Lastschriftmandats. Eine Löschung erfolgt jedoch zunächst nicht, wenn die Verarbeitung der Daten zu folgenden Zwecken weiterhin erforderlich ist:

- Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten (beispielsweise Handelsgesetzbuch, Abgabenordnung). Die dort vorgegebenen Fristen zur Aufbewahrung beziehungsweise Dokumentation betragen bis zu zehn Jahre.
- Aufbewahrung aufgrund von gesetzlichen Verjährungsvorschriften: Nach den §§ 195 ff. des Bürgerlichen Gesetzbuchs und der Verwaltungsverfahrensgesetze der Länder können diese Verjährungsfristen bis zu 30 Jahre betragen, wobei die regelmäßige Verjährungsfrist 3 Jahre beträgt.

Sofern Daten lediglich noch zu den vorgenannten Zwecken aufbewahrt werden, ist der Zugriff auf diese Daten eingeschränkt, das heißt sie stehen der Sachbearbeitung in der Regel nicht mehr zur Verfügung (Sperrung). Die Daten sind nicht mehr veränderbar und dienen ausschließlich der Aufbewahrung.
Von Dritten übermittelte Daten, die nicht innerhalb einer Frist von zwölf Monaten überprüft wurden, werden gelöscht."

(https://www.rundfunkbeitrag.de/der_rundfunkbeitrag/beitragsservice/datenschutz/datenschutz_beim_beitragseinzug/index_ger.html)

IV. Personaldatenverwaltung

Der Datenschutz für Beschäftigte des NDR hat auch im Jahr 2018 eine gewichtige Rolle gespielt. Zum einen waren Erklärungen für das sogenannte E-Recruiting von Personal anzupassen, zum anderen die Digitalisierung der Personalakten zu begleiten. Datenschutzrechtlich waren sowohl organisatorisch als auch inhaltlich Fragen zu klären, so zum Beispiel hinsichtlich

- der Vorbereitung einer Umfrage zum Sexismus im NDR,
- des Neubaus des Hauses 18a,
- des Projektes „Crossmediale Nachrichtenredaktion“ (N-Team),
- des Einsatzes von Dispositionstools zur Erstellung von Dienst- und Einsatzplänen,
- der Beauftragung eines Dienstleisters zur Analyse von Personalkosten.

Die Dienstanweisung zum Schutz personenbezogener Daten im NDR („Dienstanweisung Datenschutz“) aus dem Jahr 1996 ist bislang noch die maßgebliche interne Vorschrift des NDR zur Verarbeitung personenbezogener Daten. Diese war aufgrund der gesetzlichen Neuerungen, aber auch wegen technischer und tatsächlicher Fortschritte zu aktualisieren. Zudem gibt es einen Bedarf an einer weiteren Regelung, die eine private Randnutzung von IT-Diensten und IT-Endgeräten des NDR für Kommunikations-, Informationszwecke und Medienproduktion ermöglicht. Diesbezüglich wurde ebenfalls an einer entsprechenden Dienstanweisung gearbeitet.

Anpassungen hat es zudem gegeben in den Arbeitsverträgen des NDR: Hier waren einerseits Einwilligungserklärungen aus den Arbeitsverträgen herauszulösen, die nicht mit dem Abschluss der Verträge verknüpft sein können. Andererseits waren Regelungen zu schaffen, die als Grundlagen für Tätigkeiten der Betriebsärztin wirksam herangezogen werden können.

Weiterhin waren die Bedingungen für die sogenannten Teleheimarbeitsplätze einem eindeutigen Verfahren zuzuführen.

Eine immer wiederkehrende Frage stellte auch der regelmäßige Zugriff auf E-Mail-Accounts von Kolleg*innen dar. Derzeit – und auch zukünftig – dürfen die für jeden im NDR Beschäftigten eingerichteten E-Mail-Accounts ausschließlich für dienstliche, nicht aber für private Zwecke, genutzt werden. Aus dem umfassenden Verbot der Privatnutzung folgt, dass der Arbeitgeber ein umfassendes Zugriffsrecht auf die E-Mail-Accounts hat, etwa um stichprobenartig missbräuchliche Nutzungen zu überprüfen. Unterhalb dieser Schwelle des Prüfungsrechts des Arbeitgebers angesiedelt ist die Frage, inwieweit der Arbeitgeber vorgeben kann, ob auch andere Mitarbeiter Zugriff auf E-Mail-Accounts haben sollen. Ebenso wie bei Papierdokumenten mit dienstlichen Inhalten handelt es sich bei E-Mails nicht um private Vorgänge des jeweiligen Beschäftigten. Der Arbeitgeber (bzw. die/der Vorgesetzte) kann daher aufgrund seiner Organisationshoheit die für erforderlich gehaltenen Zugriffe definieren. Dies war in einigen Fällen nicht bekannt und führte zu Konflikten. Über den hier skizzierten Grundsatz war daher zu informieren, ebenso auch über den Umgang mit Akten, die ausschließlich zu dienstlichen Zwecken geführt werden, weshalb der Arbeitgeber organisatorisch Zugriffsrechte erteilen darf. Dabei kommt es auch nicht auf die Art der Aktenführung (Papier oder elektronisch) an.

Auch die #MeToo-Bewegung führte zu datenschutzrechtlichen Befassungen, namentlich bei der Frage nach der Gewährung von Akteneinsicht zur Überprüfung von Vorwürfen sexueller Übergriffe. Betroffene im datenschutzrechtlichen Sinne können im Falle von Akteneinsichten Personen sein, denen z.B. sexuelle Übergriffe oder Ähnliches vorgeworfen werden. Gleiches gilt für Personen, die behaupten, Opfer solcher Übergriffe geworden zu sein und Personen, die an einer Produktion beteiligt waren und deren Namen in den Akten zu erkennen sind sowie für Personen, die in den verwaltenden Bereichen einer Rundfunkanstalten die Produktion unterstützt haben und deren Namen in den Akten zu erkennen sind.

Das Recht auf informationelle Selbstbestimmung aller Betroffenen muss gewahrt werden. Zu berücksichtigen ist u. a., dass etwaig aus den Akten ersichtliche strafbare Handlungen möglicherweise bereits verjährt sind und Strafverfolgungsbehörden strafrechtliche Reaktionen verwehrt sind. Dies lässt in diesen Fällen die Unschuldsvermutung erstarken. Letztlich waren Kriterien zu entwickeln und Maßnahmen zu ergreifen, nach denen Daten von Personen, die an Produktionen beteiligt waren bzw. die in den verwaltenden Bereichen der Landesrundfunkanstalten die Produktion unterstützt haben und deren Namen in den Akten zu erkennen sind, nicht weitergegeben werden.

Nicht zuletzt wurden in zwei Schulungen die Mitarbeiter*innen der HA Personal in datenschutzrechtlichen Belangen unterrichtet, gleiches gilt auch für andere Abteilungen des NDR. Weitere Informationen für Beschäftigte wurden in Veröffentlichungen des Intranet des NDR zu allgemeinen datenschutzrechtlichen Neuerungen, aber auch zu konkreten Umsetzungsmaßnahmen zur Verfügung gestellt.

V. Sonstige Informationen

Aufgrund der vielfältigen Veröffentlichungen zur DSGVO rund um den 25. Mai 2018 hatte der Verfasser angeregt, dieses Thema auch in Leichter Sprache aufzugreifen. Der NDR bietet zu relevanten Themen derartige Beiträge an. Die Redaktion Barrierefreie Angebote und NDR Text des NDR hat dazu einen Text in Leichte Sprache übersetzt und zum Lesen oder Hören veröffentlicht (https://www.ndr.de/fernsehen/service/leichte_sprache/Leichte-Sprache-Preis-fuer-NDR-Autor-Harenberg,leichtesprache432.html).
Der Beitrag lautet wie folgt:

„Neue Regeln zum Datenschutz

Viele Firmen wissen Dinge über Sie.
Und viele Behörden wissen Dinge über Sie.
Zum Beispiel:

- Ihren Geburtstag.
- Oder Ihre Adresse.

Auch viele Menschen wissen Dinge über Sie.

- Ihr Arzt kennt zum Beispiel Ihre Krankheiten.
- Und Ihr Chef kennt Ihr Gehalt.

Diese Dinge über Sie heißen Daten.
Und diese Daten sind geschützt.
Das heißt:
Niemand darf Ihre Daten ohne Grund speichern.
Und niemand darf Ihre Daten ohne Ihre Erlaubnis weitersagen.
Dafür gibt es ein Wort.
Dieses Wort ist Datenschutz.

Zum Datenschutz gibt es jetzt neue Regeln.
Diese Regeln sind von der Europäischen Union.

Die Europäische Union ist eine Gruppe von Ländern.

In dieser Gruppe sind 28 Länder in Europa.

Die Abkürzung für Europäische Union ist EU.

Mit diesen Regeln will die EU die Daten von Menschen noch besser schützen.
Diese Regeln heißen Datenschutz·grundverordnung.
Die Abkürzung für Datenschutz·grundverordnung ist DSGVO.

Die neuen Regeln
An die neuen Regeln müssen sich alle Behörden in Europa halten.
Und alle Firmen.
Die neuen Regeln gelten aber zum Beispiel auch für amerikanische Firmen.
Zum Beispiel für Facebook.
Oder für Google.
Facebook und Google sammeln nämlich viele Daten von vielen Menschen.
Auch in Europa.

Wir schreiben ab jetzt immer nur Firmen.

Aber wir meinen damit auch Behörden.

Firma muss um Erlaubnis fragen
Will eine Firma Daten von einem Menschen aus der EU speichern?
Und will die Firma mit diesen Daten etwas machen?
Zum Beispiel:
Will die Firma diese Daten an eine andere Firma weitergeben?
Dann muss die Firma diesen Menschen um Erlaubnis fragen.
Und dieser Mensch muss die Erlaubnis geben.
Ist dieser Mensch jünger als 16 Jahre?
Dann muss ein Erziehungs·berechtigter die Erlaubnis geben.

Ein Erziehungs·berechtigter ist verantwortlich für einen Menschen.

Erziehungs·berechtigte sind meistens die Eltern.

Die Firma muss auch sagen:

Das machen wir mit Ihren Daten.

Und so lange speichern wir Ihre Daten.

Firma muss antworten

Fragt ein Mensch aus der EU eine Firma:

Welche Daten von mir haben Sie gespeichert?

Und warum haben Sie Daten von mir gespeichert?

Dann muss die Firma auf diese Fragen antworten.

Firma muss Daten löschen

Hat eine Firma Daten von einem Menschen aus der EU gespeichert?

Aber dieser Mensch hat keine Erlaubnis gegeben?

Oder es gibt keinen Grund mehr für die Speicherung?

Dann muss die Firma die Daten löschen.

Hält sich die Firma nicht an alle neuen Regeln?

Dann muss die Firma eine hohe Strafe bezahlen."

Das Vorhaben war erfolgreich: Der Autor Herr Mark Harenberg wurde für diese Übersetzung mit dem Leichte-Sprache-Preis der Universität Hildesheim und der Dudenredaktion ausgezeichnet.

VI. Organisations- und Strukturprojekte

Eine Reihe von Projekten, teilweise in Mitbestimmungsverfahren, in sonstigen Anfragen oder Einzelanforderungen waren datenschutzrechtlich zu bewerten. So wurden rund 50 „kleinere" neue Softwareanwendungen zum Einsatz gebracht. Auch die weiteren Anfragen und Projekte waren vielfältig: So ging es etwa um die Ablösung und den Ersatz von ISDN-Telefonen, um technische Ausstattungen des NDR im Plenarsaal des Landtags Schleswig-Holstein, um neue Mess-, Übertragungs- und Reporterwagen, Tools zur Planung von Veranstaltungen, elektronische Schlüsselverwaltungssysteme, die Möglichkeit der Nutzung von Clouds in unterschiedlichen Zusammenhängen, den Einsatz von Zahlungsverkehrssoftwaren, Regieplätze für das Live-Streaming-Regieplatz Online NDS, mobile Sendeabwicklungen, NDR Musik- und Filmförderungen, den Ersatz von Web-Analyse-Systemen, ein Newsroom Management System und Regelungen für Messenger-Dienste und Customer-Relationship-Managementsysteme.

Von besonderer Bedeutung war und ist der anstehende Einsatz von Windows 10 aus datenschutzrechtlicher Sicht. Nach den Erkenntnissen aus dem Ende des Jahres 2018 musste davon ausgegangen werden, dass Microsoft planmäßig und umfangreich Daten

über individuelle Nutzungen sammelt, ohne dass die Nutzer*innen dies bemerken und ohne die Möglichkeit, diese Datenerfassungen auszuschalten oder einzusehen, welche Daten gesammelt werden. Weiterhin setzt Microsoft eine Software ein, die regelmäßig Telemetriedaten an eigene Server in den USA sendet. Microsoft sammelt dabei nicht nur Nutzungsdaten über den eingebauten Telemetrie-Client, sondern erfasst und speichert auch die individuelle Nutzung von Connected Services (Stand November 2018). Das Bundesamt für die Sicherheit in der Informationstechnik hatte am 20. November 2018 Folgendes veröffentlicht (abrufbar unter https://www.bsi.bund.de/DE/Presse/ Pressemitteilungen/Presse2018/Studie_Win_10_20112018.html - letzter Abruf am 18.02.2018):

„Das Betriebssystem Windows 10 sendet umfangreiche System- und Nutzungsinformationen an Microsoft. Eine Unterbindung der Erfassung und Übertragung von Telemetriedaten durch Windows ist technisch zwar möglich, für Anwender aber nur schwer umzusetzen. Das ist das Ergebnis einer Untersuchung der zentralen Telemetriekomponente von Windows 10, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt hat. Die Untersuchung der Telemetriekomponente ist Teil einer umfangreichen Sicherheitsanalyse, in der das BSI sicherheitskritische Funktionen des Betriebssystems untersucht. Ziel ist es, die Sicherheit und Restrisiken für eine Nutzung von Windows 10 bewerten zu können, Rahmenbedingungen für einen sicheren Einsatz des Betriebssystems zu identifizieren sowie praktisch nutzbare Empfehlungen für eine Härtung und den sicheren Einsatz von Windows 10 zu erstellen. Informationen zur Studie sowie die ersten Teilergebnisse sind auf der Webseite des BSI abrufbar.

‚Als nationale Cyber-Sicherheitsbehörde ist es Aufgabe des BSI, Anwender in Staat, Wirtschaft und Gesellschaft dabei zu unterstützen, IT-Produkte und Software sicher einsetzen zu können. Mehr als ein Drittel der Computernutzer weltweit setzt Windows 10 ein, Tendenz steigend. Daher prüfen wir das Betriebssystem auf Herz und Nieren und leiten daraus im Sinne eines digitalen Verbraucherschutzes konkrete Empfehlungen ab, mit denen die Digitalisierung ein Stück sicherer wird‘, erklärt Arne Schönbohm, Präsident des BSI.

Den Analysen zufolge hat die in Windows 10 >ab Werk< eingebaute Telemetriekomponente umfassende Möglichkeiten, auf System- und Nutzungsinformationen zuzugreifen und diese an den Hersteller zu versenden. Obwohl die Nutzer unterschiedliche Telemetrielevel einstellen können, ordnet der Telemetriedienst die vorhandenen

Telemetriequellen diesen Leveln im laufenden Betrieb dynamisch zu. Hierfür lädt der Dienst mehrmals pro Stunde Konfigurationsdaten nach. Eine Unterbindung der Erfassung und Übertragung von Telemetriedaten durch Windows ist technisch zwar möglich, für den einfachen Anwender allerdings nur schwer umzusetzen. Zudem haben auf dem Rechner installierte Anwendungen wie der Internet Explorer und Microsoft Office die Möglichkeit, auch ohne den zentralen Telemetriedienst des Betriebssystems Telemetriedaten zu erfassen und an den Hersteller zu versenden."

Anhaltspunkte dafür, dass datenschutzrechtliche Grundsätze nicht eingehalten werden, lagen daher im Berichtsjahr aus den genannten Gründen vor. Der NDR hat allerdings in der Folgezeit Abhilfemaßnahmen getroffen. Zudem hat Microsoft angekündigt, bis April 2019 Optionen anzubieten, um die Sammlung von Telemetriedaten zu beschränken und den Vorgaben der DSGVO Rechnung zu tragen.

Gleiches galt auch bezüglich des Einsatzes von Office 365. Auch diesbezüglich lagen im Berichtszeitraum Anhaltspunkte vor, dass die derzeitige Funktionalität von Office 365 nicht den Vorgaben der DSGVO entspricht. Die Bewertungen von Windows 10 und Office 365 waren im Jahr 2018 noch nicht abgeschlossen. Die Fortsetzungen hierzu folgen also in dem Bericht für das Jahr 2019.

VII. Verbreitungsfragen

Hinsichtlich der Zurverfügungstellung der Programmangebote des NDR standen Fragen bei der Verbreitung der vom NDR verantworteten Telemedienangebote und die Nutzung von Sprachassistenten im Vordergrund.

Nach einer Veröffentlichung der Zeitschrift Stiftung Warentest mit dem Titel „TV Mediatheken/Den Zuschauer im Blick" soll auch die NDR Hamburg App (NDR 90,3 und Hamburg Journal) „kritisch" sein, weil „Daten gesendet wurden, die für den Betrieb der App nicht notwendig" seien. Damit wurde der Eindruck erweckt, dass eine Übermittlung personenbezogener Daten der Nutzer*innen beim Betrieb erfolgt. Dies war und ist allerdings nicht der Fall. Datenschutzrechtlich sind die Befunde nicht zu beanstanden: In Messungen des NDR konnte nachvollzogen werden, dass übermittelte Daten wie z. B. der Mobilfunkbetreiber im Rahmen eines externen Push-Services benötigt werden. Gleichwohl hat der NDR Maßnahmen ergriffen, um auch diese Daten zu reduzieren.

Soweit in dem Artikel weiterhin ausgeführt wird, dass die NDR Hamburg App nicht „verschwiegen“ und daher nicht „harmlos“ sei (und überdies Ausführungen macht wie „Das Ende der Unschuld – Der Komfort hat Folgen.“ und „Niemand sieht, was ich sehe – mit dieser Anonymität ist es vorbei.“), werden diese Behauptungen nur am Rande kassiert: „Daten mit direktem Rückschluss auf konkrete Personen fanden wir aber nicht.“ Und weiter: „Zum Spion ist der schlaue Fernseher nicht mutiert. Personenbezogene Daten sendet er nicht ins Internet.“

Eine Verletzung datenschutzrechtlicher Vorgaben konnte daher nicht festgestellt werden.

Soweit die Telemedienangebote des NDR noch nicht vollständig die https-Verschlüsselung für alle Internetseiten nutzt, besteht Nachholbedarf. Zwar sollen die Umsetzungsmaßnahmen unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Aufgrund der Implementierungskosten, auch bedingt durch den dafür erforderlichen Personaleinsatz, ist es noch zu keiner vollständigen Umsetzung gekommen. Gleichwohl sind die Anstrengungen zu forcieren.

Problematisch ist weiterhin der Einsatz von Sprachassistenten zur Verbreitung der Programme. Dies gilt sowohl bezüglich der Nutzung durch das Publikum, als auch für den internen Gebrauch im NDR. Sprachassistenten können durch das „Mithören“ auch den Persönlichkeitsbereich von Beschäftigten berühren. Denn was mit Sprachassistenten kommuniziert wird, dürfte regelmäßig aufgezeichnet werden: Die Geräte schicken die Aufzeichnungen in Form von Audiodateien in Clouds, die sich regelmäßig auf Servern im Ausland befinden können. Die Daten können daher auf Servern in Ländern gelangen, die einem geringeren Datenschutzstandard als in Deutschland unterliegen. Unter anderem ist auch ein Zugriff von Geheimdiensten nicht ausgeschlossen. Eine Übermittlung personenbezogener Daten in das außereuropäische Ausland ist aber nur dann zulässig, wenn in dem Land, in das die Daten übermittelt werden, ein vergleichbar hohes Datenschutzniveau besteht. Diesbezüglich ist die weitere Rechtsprechung abzuwarten: So besteht zum Beispiel ein nicht geringes Risiko, dass auch der Angemessenheitsbeschluss der EU-Kommission zum sog. Privacy Shield vom Europäischen Gerichtshof ebenso für unwirksam erklärt wird, wie vor einiger Zeit das sog. Safe-Harbor-Abkommen. Damit könnten Datenübermittlungen in die USA unzulässig werden.

VIII. Zusammenarbeit mit anderen Datenschutzbeauftragten

Die Zusammenarbeit mit anderen datenschutzrechtlichen Aufsichtsbehörden ist gesetzlich vorgeschrieben und aufgrund der Fülle der zu erledigenden Aufgaben auch sinnvoll. Daher gab es auch im Jahr 2018 einen stetigen und produktiven Austausch, insbesondere im AKDSB.

1. AKDSB

Die Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradio (AKDSB) haben sich auch im Berichtsjahr 2018 zweimal zu Präsenzsitzungen getroffen. Darüber hinaus gab es aufgrund der zahlreichen Neuregelungen weiteren Beratungsbedarf, der eine Sondersitzung sowie Telefonschaltkonferenzen erforderlich machte. Themenschwerpunkte des AKDSB waren:

- Der Rundfunkteilnehmerdatenschutz, und hier namentlich das Projekt des Zentralen Beitragsservice (ZBS) zur Umsetzung der Datenschutzgrundverordnung, Löschkonzepte, datenschutzrechtliche Aspekte aufgrund der Entscheidung des BVerfG zur Verfassungsmäßigkeit des Rundfunkbeitrags mit Ausnahme der Nebenwohnungen, die Vorbereitungsarbeiten beim ZBS für den Meldedatenabgleich 2018 sowie die Umsetzung des Auskunftsanspruches nach Art. 15 DSGVO.
- Die aktuelle Datenschutzgesetzgebung und –politik hat ebenfalls Beratungsbedarf ausgelöst, etwa auch mit Blick auf die ePrivacy-Verordnung und die strittige Frage der Fortgeltung des TMG.
- Regen Austausch gab es überdies zur Umsetzung DSGVO in den Rundfunkanstalten, dies mit Blick auf die organisatorischen Vorgaben die materiellen Anforderungen der DSGVO. Gegenstand der Beratungen waren beispielsweise das Verzeichnis der Verfahrenstätigkeiten, Muster zur Auftragsverarbeitung, die Anpassung sonstiger Verträge, die Umsetzung der Verpflichtung der Beschäftigten auf die Vertraulichkeit, Videoüberwachungen.
- Weitere Schwerpunkte waren die Konsequenzen aus dem EuGH-Urteil zu Facebook Fanpages, der zukünftige Umgang mit Nutzungsmessung bei Telemedienangeboten, datenschutzrechtliche Fragen bei HbbTV-Angeboten, Akkreditierungsforderungen bei Sportveranstaltungen, Harmonisierungsprojekte im Rahmen des Prozesses „Auftrag und Strukturoptimierung“, der Datenschutz beim IVZ. Auch die Strukturierung des AKDSB selbst war zu erörtern.

2. Das virtuelle Datenschutzbüro

Der Rundfunkdatenschutzbeauftragte hat sich auch im Berichtsjahr 2018 als sogenannter Projektpartner an dem vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) technisch bereitgestellten „Virtuellen Datenschutzbüro“ (VirDSB) beteiligt. Das VirDSB ist ein gemeinsamer Service, der von überwiegend deutschen Datenschutzinstitutionen im Internet (http:/ /www.datenschutz.de) angeboten wird. Es werden Informationen über datenschutzrechtliches Grundwissen für Bürger*innen und Expert*innen dargeboten. Die Internetseite des Rundfunkdatenschutzbeauftragten verlinkt auf diese Seite.

An der Sitzung der Projektpartner des Virtuellen Datenschutzbüros am 06. März 2018 in Hannover hat der Rundfunkdatenschutzbeauftragte des NDR teilgenommen. Von besonderer Bedeutung war die Schaffung einer neuen Geschäftsordnung für das Virtuelle Datenschutzbüro. Der Rundfunkdatenschutzbeauftragte des NDR hatte diese Aufgabe gemeinsam mit der Geschäftsführung übernommen.

3. Zusammenarbeit mit anderen Aufsichtsbehörden auf nationaler Ebene

Auch nach alter Rechtslage war es Aufgabe der deutschen Datenschutzkontrollstellen und –aufsichtsbehörden zusammenzuarbeiten (Art. 28 Abs. 6 Satz 3 EG-Datenschutzrichtlinie und § 26 Abs. 4 BDSG alt). Der Gesetzgeber hat diese Pflicht erneut im novellierten § 18 Abs. 1 Satz 4 BDSG festgeschrieben. Danach sollen alle Aufsichtsbehörden beteiligt werden, wenn diese Aufsichtsbehörden von einer entsprechenden Angelegenheit betroffen sind.

Eine solche Betroffenheit ist bei einer Vielzahl von Angelegenheiten der Rundfunkanstalten gegeben. Überdies ist der Rundfunkdatenschutzbeauftragte auch Aufsichtsbehörde über die Beteiligungsunternehmen des NDR, so dass es kaum datenschutzrechtliche Themenbereiche gibt, die keine Relevanz für den Zuständigkeitsbereich des Rundfunkdatenschutzbeauftragten entfalten würden. Gleichwohl haben nach wie vor die Landesdatenschutzbeauftragten ihren Kreis nicht erweitern wollen. So heißt es noch immer auf der Internetpräsenz der Datenschutzkonferenz:

„Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren

und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen“ (https://www.datenschutzkonferenz-online.de/dsk.html). Trotz wiederholter Versuche der Datenschutzbeauftragten der Rundfunkanstalten wird eine Aufnahme der Rundfunkdatenschutzbeauftragten, aber auch der Datenschutzbeauftragten der Kirchen, verweigert. Das soeben abgebildete Zitat der Datenschutzkonferenz zur Zusammensetzung dieser bildet daher nicht gesetzlich geforderten Zustand ab, weil nicht alle Aufsichtsbehörden in die Konferenz einbezogen werden.

F. Ausblick

Wie erwartet, hat die Datenschutzgrundverordnung in allen Bereichen des NDR Befassungsaufwand ausgelöst. Die immer aktuell zu haltenden und zu überprüfenden gesetzlichen Anforderungen werden stetig aufgrund der Dokumentations- und Nachweispflichten Verwaltungsbefassung nach sich ziehen und Beratungsbedarf mit sich bringen. Hinzu kommt weitere Gesetzgebung und die andauernde Digitalisierung von Geschäftsabläufen sowie Umstrukturierungen, auch ausgelöst durch die „Strukturoptimierung des öffentlich-rechtlichen Rundfunks im digitalen Zeitalter“, und der sich daraus ergebenden Betroffenheit der Verwaltung, Technik, IT und Produktion des NDR.

Datenschutz, also der Schutz der informationellen Selbstbestimmung erfährt unter den Bedingungen der Digitalisierung eine herausgehobene Stellung. Denn die Digitalisierung birgt bekanntlich sowohl Chancen als auch Risiken – und sogar Gefahren. Nur eines ist sicher: Man muss aufpassen.

Teil B – Anlagen: Auszüge aus wesentlichen gesetzlichen Grundlagen

Auszug aus der Datenschutzgrundverordnung

Artikel 4 – Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8.„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9.„Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10.„Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

11.„Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

12.„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

13.„genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

14.„biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

15.„Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

16.„Hauptniederlassung“

a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;
b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat

den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

17. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

18. „Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

19. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

20. „verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern;

21. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle;

22. „betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

    a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,
    b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder
    c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

23. „grenzüberschreitende Verarbeitung“ entweder

    a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder
    b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

24. „maßgeblicher und begründeter Einspruch“ einen Einspruch gegen einen Beschlussentwurf im

Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

25. „Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates;

26. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Artikel 5 – Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 6 – Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und

nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Artikel 7 – Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Artikel 8 – Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.
Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

(2) Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

(3) Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

Artikel 9 – Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,
c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,
d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßi-

gen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Artikel 13 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

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

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) 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:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) 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 Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Artikel 15 – Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;
b) die Kategorien personenbezogener Daten, die verarbeitet werden;
c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Artikel 16 – Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

Artikel 17 – Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist
a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Artikel 18 – Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

Artikel 19 – Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Artikel 20 – Recht auf Datenübertragbarkeit

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und
b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Artikel 21 – Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(4) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(5) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

(6) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

Artikel 22 - Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die

ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Artikel 24 – Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B.

Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Artikel 26 – Gemeinsam für die Verarbeitung Verantwortliche

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Artikel 28 – Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung

anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) 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. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei

insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Artikel 30 - Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands

oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Artikel 35 - Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Artikel 51 – Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde“).

(2) Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII zusammen.

(3) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im Ausschuss vertritt, und führt ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 einhalten.

(4) Jeder Mitgliedstaat teilt der Kommission bis spätestens 25. Mai 2018 die Rechtsvorschriften, die er aufgrund dieses Kapitels erlässt, sowie unverzüglich alle folgenden Änderungen dieser Vorschriften mit.

Artikel 52 – Unabhängigkeit

(1) Jede Aufsichtsbehörde handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Verordnung völlig unabhängig.

(2) Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.

(3) Das Mitglied oder die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.

(4) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.

(5) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihr eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.

(6) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt und dass sie über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

Artikel 53 – Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird, und zwar

- vom Parlament,
- von der Regierung,
- vom Staatsoberhaupt oder
- von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird.

(2) Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.

(3) Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder verpflichtender Versetzung in den Ruhestand gemäß dem Recht des betroffenen Mitgliedstaats.

(4) Ein Mitglied wird seines Amtes nur enthoben, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt.

Artikel 54 - Errichtung der Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften Folgendes vor:

a) Errichtung jeder Aufsichtsbehörde;
b) die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied jeder Aufsichtsbehörde;
c) die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde;
d) die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde von mindestens vier Jahren; dies gilt nicht für die erste Amtszeit nach 24. Mai 2016, die für einen Teil der

Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist;

e) die Frage, ob und — wenn ja — wie oft das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können;

f) die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.

(2) Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während dieser Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstößen gegen diese Verordnung.

Artikel 55 – Zuständigkeit

(1) Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.

(2) Erfolgt die Verarbeitung durch Behörden oder private Stellen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe c oder e, so ist die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig. In diesem Fall findet Artikel 56 keine Anwendung.

(3) Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

Artikel 57 – Aufgaben

(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

a) die Anwendung dieser Verordnung überwachen und durchsetzen;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;

c) im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;

d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren;

e) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;

f) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unter-

richten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;

h) Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

i) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;

j) Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 und des Artikels 46 Absatz 2 Buchstabe d festlegen;

k) eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß Artikel 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;

l) Beratung in Bezug auf die in Artikel 36 Absatz 2 genannten Verarbeitungsvorgänge leisten;

m) die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Absatz 1 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 bieten müssen, Stellungnahmen abgeben und sie billigen;

n) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen;

o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig überprüfen;

p) die Kriterien für die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;

q) die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 vornehmen;

r) Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 genehmigen;

s) verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;

t) Beiträge zur Tätigkeit des Ausschusses leisten;

u) interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 ergriffene Maßnahmen und

v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(2) Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und gegebenenfalls für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anfragen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In

diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

Artikel 58 – Befugnisse

(1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

a) den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,
c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,
d) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,
e) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,
f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,
a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,
b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,
c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,
d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen,
f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,
h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,
i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,
j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

(3) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,

a) gemäß dem Verfahren der vorherigen Konsultation nach Artikel 36 den Verantwortlichen zu beraten,
b) zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,
c) die Verarbeitung gemäß Artikel 36 Absatz 5 zu genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,
d) eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln gemäß Artikel 40 Absatz 5 zu billigen,
e) Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren,
f) im Einklang mit Artikel 42 Absatz 5 Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen,
g) Standarddatenschutzklauseln nach Artikel 28 Absatz 8 und Artikel 46 Absatz 2 Buchstabe d festzulegen,
h) Vertragsklauseln gemäß Artikel 46 Absatz 3 Buchstabe a zu genehmigen,
i) Verwaltungsvereinbarungen gemäß Artikel 46 Absatz 3 Buchstabe b zu genehmigen
j) verbindliche interne Vorschriften gemäß Artikel 47 zu genehmigen.

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.

(5) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen.

(6) Jeder Mitgliedstaat kann durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2 und 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen.

Artikel 85 - Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

(1) Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.

(2) Für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehör-

den), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

(3) Jeder Mitgliedstaat teilt der Kommission die Rechtsvorschriften, die er aufgrund von Absatz 2 erlassen hat, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.

Staatsvertrag über den Datenschutz beim Norddeutschen Rundfunk (NDR-Datenschutz-Staatsvertrag)

§ 1 – Datenverarbeitung zu journalistischen Zwecken, Medienprivileg

(1) Soweit der NDR personenbezogene Daten zu journalistischen Zwecken verarbeitet, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen Zwecken von der Verordnung (EU) 2016/679 außer den Kapiteln I, VIII, X und XI nur die Artikel 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Artikel 24 und Artikel 32 Anwendung. Die Artikel 82 und 83 der Verordnung (EU) 2016/679 gelten mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses gemäß den Sätzen 1 bis 3 sowie für unzureichende Maßnahmen nach Artikel 5 Abs. 1 Buchst. f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Die Sätze 1 bis 5 gelten entsprechend für die Datenverarbeitung zu journalistischen Zwecken der Hilfs- und Beteiligungsunternehmen des NDR. Der NDR kann sich einen Verhaltenskodex geben, der in einem transparenten Verfahren erlassen und veröffentlicht wird. Den betroffenen Personen stehen nur die in den Absätzen 2 und 3 genannten Rechte zu.

(2) Führt die journalistische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, kann die betroffene Person Auskunft über die der Berichterstattung zugrunde liegenden zu ihrer Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann oder
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Die betroffene Person kann die unverzügliche Berichtigung unrichtiger personenbezogener Daten im Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Die weitere Speicherung der personenbezogenen Daten ist rechtmäßig, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen erforderlich ist.

§ 2 – Ernennung der oder des Rundfunkdatenschutzbeauftragten

(1) Der NDR ernennt eine Beauftragte oder einen Beauftragten für den Datenschutz beim NDR (Rundfunkdatenschutzbeauftragte oder Rundfunkdatenschutzbeauftragter), die oder der zuständige Aufsichtsbehörde im Sinne des Artikels 51 der Verordnung (EU) 2016/679 ist. Die Ernennung erfolgt durch den Rundfunkrat auf Vorschlag des Verwaltungsrats für die Dauer von vier Jahren. Eine dreimalige Wiederernennung ist zulässig. Die oder der Rundfunkdatenschutzbeauftragte muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Das Amt der oder des Rundfunkdatenschutzbeauftragten kann nicht neben anderen Aufgaben innerhalb des NDR und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt der oder des Rundfunkdatenschutzbeauftragten zu vereinbaren sein und dürfen ihre oder seine Unabhängigkeit nicht gefährden.

(2) Das Amt endet mit Ablauf der Amtszeit, mit Rücktritt vom Amt oder mit Erreichen des gesetzlichen Renteneintrittsalters. Tarifvertragliche Regelungen bleiben unberührt. Die oder der Rundfunkdatenschutzbeauftragte kann ihres oder seines Amtes nur enthoben werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Verwaltungsrates auf Vorschlag des Rundfunkrates; die oder der Rundfunkdatenschutzbeauftragte ist vor der Entscheidung zu hören.

(3) Das Nähere, insbesondere die Grundsätze der Vergütung, beschließt der Verwaltungsrat mit Zustimmung des Rundfunkrates in einer Satzung.

§ 3 – Unabhängigkeit der oder des Rundfunkdatenschutzbeauftragten

(1) Die oder der Rundfunkdatenschutzbeauftragte ist in Ausübung ihres oder seines Amtes unabhängig und nur dem Gesetz unterworfen. Sie oder er unterliegt keiner Rechts- oder Fachaufsicht. Der Dienstaufsicht des Verwaltungsrates untersteht sie oder er nur insoweit, als ihre oder seine Unabhängigkeit bei der Ausübung ihres oder seines Amtes dadurch nicht beeinträchtigt wird.

(2) Die Dienststelle der oder des Rundfunkdatenschutzbeauftragten wird bei der Geschäftsstelle von Rundfunkrat und Verwaltungsrat eingerichtet. Der oder dem Rundfunkdatenschutzbeauftragten ist die für die Erfüllung ihrer oder seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen. Die erforderlichen Mittel sind jährlich, öffentlich und gesondert im Haushaltsplan des NDR auszuweisen und der oder dem Rundfunkdatenschutzbeauftragten im Haushaltsvollzug zuzuweisen. Einer Finanzkontrolle durch den Verwaltungsrat unterliegt die oder der Rundfunkdatenschutzbeauftragte nur insoweit, als ihre oder seine Unabhängigkeit bei der Ausübung ihres oder seines Amtes dadurch nicht beeinträchtigt wird.

(3) Die oder der Rundfunkdatenschutzbeauftragte ist in der Wahl ihrer oder seiner Mitarbeiterinnen oder Mitarbeiter frei. Sie unterstehen allein ihrer oder seiner Leitung.

§ 4 – Aufgaben und Befugnisse der oder des Rundfunkdatenschutzbeauftragten

(1) Die oder der Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften dieses Staatsvertrages, des Rundfunkstaatsvertrages, der Verordnung (EU) 2016/679 und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des NDR und seiner Beteiligungsunternehmen im Sinne des § 16c Abs. 3 Satz 1 RStV. Sie oder er hat die Aufgaben und Befugnisse entsprechend der Artikel 57 und 58 Abs. 1 bis 5 der Verordnung (EU) 2016/679. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden hat sie oder er, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, den Informantenschutz zu wahren. Sie oder er kann gegenüber dem NDR keine Geldbußen verhängen.

(2) Stellt die oder der Rundfunkdatenschutzbeauftragte Verstöße gegen Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber der Intendantin oder dem Intendanten und fordert sie oder ihn zur Stellungnahme innerhalb einer angemessenen Frist auf. Gleichzeitig unterrichtet sie oder er den Verwaltungsrat. Von einer Beanstandung und Unterrichtung kann abgesehen werden, wenn es sich um unerhebliche Mängel handelt, oder wenn ihre unverzügliche Behebung sichergestellt ist.

(3) Die von der Intendantin oder dem Intendanten nach Absatz 2 Satz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Rundfunkdatenschutzbeauftragten getroffen worden sind. Die Intendantin oder der Intendant leitet dem Verwaltungsrat gleichzeitig eine Abschrift der Stellungnahme gegenüber der oder dem Rundfunkdatenschutzbeauftragten zu.

(4) Die oder der Rundfunkdatenschutzbeauftragte erstattet jährlich auch den Organen des NDR den schriftlichen Bericht im Sinne des Artikels 59 der Verordnung (EU) 2016/679 über ihre oder seine Tätigkeit. Der Bericht wird veröffentlicht, wobei eine Veröffentlichung im Online-Angebot des NDR ausreichend ist.

(5) Jedermann hat das Recht, sich unmittelbar an die Rundfunkdatenschutzbeauftragte oder den Rundfunkdatenschutzbeauftragten zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den NDR oder seiner Beteiligungsunternehmen im Sinne des Absatzes 1 Satz 1 in seinen schutzwürdigen Belangen verletzt zu sein.

(6) Die oder der Rundfunkdatenschutzbeauftragte ist sowohl während als auch nach Beendigung ihrer oder seiner Tätigkeit verpflichtet, über die ihr oder ihm während ihrer oder seiner Dienstzeit bekannt gewordenen Angelegenheiten und vertraulichen Informationen Verschwiegenheit zu bewahren.

Satzung über die oder den Rundfunkdatenschutzbeauftragte/n beim Norddeutschen Rundfunk

In Ausführung des § 2 Absatz 3 des Staatsvertrags über den Datenschutz beim Norddeutschen Rundfunk vom 25.05.2018 (NDR-Datenschutz-Staatsvertrag) hat der Verwaltungsrat mit Beschluss vom 18.05.2018 und mit Zustimmung des Rundfunkrats vom 25.05.2018 die nachstehende Satzung erlassen:

I. Aufgaben der/des Rundfunkdatenschutzbeauftragten

Artikel 1 – Stellung der/des Rundfunkbeauftragten für Datenschutz

1. Die/der Rundfunkdatenschutzbeauftragte ist unabhängige Aufsichtsbehörde im Sinne der Art. 51 ff der Verordnung (EU) 2016/679 (DSGVO). Sie/er nimmt ihre/ seine Aufgaben und Befugnisse unabhängig wahr, um den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

2. Die/der Rundfunkdatenschutzbeauftragte überwacht die Einhaltung der Vorschriften über den Datenschutz, insbesondere der DSGVO, im NDR und seinen Hilfs- und Beteiligungsunternehmen. Sie/er leistet einen Beitrag zur einheitlichen Anwendung der DSGVO in der gesamten Europäischen Union und bei den öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland.

Artikel 2 - Aufgaben der/des Rundfunkdatenschutzbeauftragten

1. Die/der Rundfunkdatenschutzbeauftragte hat insbesondere folgende Aufgaben:

    a. die Anwendung der Vorschriften über den Datenschutz zu überwachen und durchzusetzen;
    b. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;
    c. im Einklang mit dem geltenden Recht den NDR, seine Hilfs- und Beteiligungsunternehmen und Gremien über Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten;
    d. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten zu sensibilisieren;
    e. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund der Vorschriften über den Datenschutz zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit anderen Aufsichtsbehörden zusammenzuarbeiten;
    f. sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
    g. mit anderen Aufsichtsbehörden unter Wahrung der medienfreiheitimmanenten Grenzen zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung der Vorschriften über Datenschutz zu gewährleisten;

h. Untersuchungen über die Anwendung der DSGVO durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;
i. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;
j. Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 DSGVO und des Artikels 46 Absatz 2 Buchstabe d DSGVO festzulegen;
k. eine Liste der Verarbeitungsarten zu erstellen und zu führen, für die gemäß Artikel 35 Absatz 4 DSGVO eine Datenschutzfolgenabschätzung durchzuführen ist;
l. Beratung in Bezug auf die in Artikel 36 Absatz 2 DSGVO genannten Verarbeitungsvorgänge zu leisten;
m. die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 DSGVO zu fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 DSGVO bieten müssen, Stellungnahmen abzugeben und sie zu billigen;
n. Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 DSGVO zu genehmigen;
o. verbindliche interne Vorschriften gemäß Artikel 47 DSGVO zu genehmigen;
p. interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 DSGVO ergriffene Maßnahmen zu erstellen und
q. jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten zu erfüllen.

2. Die/der Rundfunkdatenschutzbeauftragte erleichtert das Einreichen von in Artikel 2 Ziffer 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

3. Die Bearbeitung von Anfragen und Beschwerden durch die/den Rundfunkdatenschutzbeauftragte/n ist unentgeltlich.

4. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen (bspw. mehr als ein Antrag pro Quartal etc.) kann die/der Rundfunkdatenschutzbeauftragte eine angemessene Gebühr auf der Grundlage der Verwaltungskosten gemäß dem Justizvergütungs- und –entschädigungsgesetz (JVEG) in seiner jeweils geltenden Fassung verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall trägt die/der Rundfunkdatenschutzbeauftragte die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter des Antrags.

5. Die /der Rundfunkdatenschutzbeauftragte erstattet dem Verwaltungsrat jährlich einen Tätigkeitsbericht neben den Anforderungen aus § 4 Absatz 4 NDR-Datenschutz-Staatsvertrag.
6. Die Dienststelle der/des Rundfunkdatenschutzbeauftragten lautet:
   Norddeutscher Rundfunk
   Rundfunkbeauftragte/r für Datenschutz
   Gremienbüro
   Rothenbaumchaussee 132, 20149 Hamburg

II. Grundsätze der Vergütung der/des Rundfunkdatenschutzbeauftragten

Artikel 3

1. Die Festlegung der Vergütung erfolgt durch den Verwaltungsrat für die Dauer der Amtszeit der/des Rundfunkdatenschutzbeauftragten.
2. Die Festlegung der Vergütung erfolgt mindestens nach Maßgabe der Vergütungsgruppe 2 des Tarifvertrags über die Vergütungsordnung des NDR, wobei die fachliche und persönliche Eignung der/des Rundfunkdatenschutzbeauftragten zu berücksichtigen ist.
3. Der Verwaltungsrat genehmigt den Bedarf für die Personal-, Finanz- und Sachausstattung der/des Rundfunkdatenschutzbeauftragten und übt die Finanzkontrolle unter Berücksichtigung der Unabhängigkeit des Amtes aus.

III. Satzungsänderung

Artikel 4

1. Die Satzung kann durch Beschluss des Verwaltungsrats mit einfacher Mehrheit und Zustimmung des Rundfunkrats geändert werden.
2. Der Rundfunkrat kann Änderungen der Satzung vorschlagen.

IV. Inkrafttreten der Satzung

Artikel 5

1. Diese Satzung tritt mit Zustimmung des Rundfunkrats am 25.05.2018 in Kraft.
2. Sie wird in den Mitteilungsblättern der Länder Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein bekannt gegeben.