17/18

BERICHT DER DATENSCHUTZ BEAUFTRAGTEN

2017/2018

AUFGESTELLT GEMÄSS § 51 ABSATZ 5 WDR-GESETZ

25. BERICHT DER DATENSCHUTZBEAUFTRAGTEN 2017/2018

Inhaltsverzeichnis

1. Vorwort, Aufgaben und Befugnisse

1.1. Datenschutzbeauftragte…

In seiner 580. Sitzung am 30. Juni 2016 in Köln bestellte mich der Rundfunkrat bei 40 anwesenden Mitgliedern einstimmig und ohne Enthaltung auf Vorschlag des Intendanten vom 1. August 2016 bis 31. Juli 2020 zur Beauftragten für den Datenschutz gemäß § 53 Absatz 1 WDR-Gesetz alte Fassung. Damit bin ich für den WDR aufsichtsrechtlich an die Stelle der Landesbeauftragten für den Datenschutz getreten. Gleichzeitig nehme ich gemäß § 53 Absatz 2 WDR-Gesetz alte Fassung die Aufgaben einer behördlichen Datenschutzbeauftragten nach § 32a des Datenschutzgesetzes Nordrhein-Westfalen alte Fassung wahr.

Mit der Neufassung des WDR-Gesetzes vom 25. April 2018 hat sich der nordrhein-westfälische Gesetzgeber entschlossen, die Aufgaben der Aufsichtsbehörde und die der Datenschutzbeauftragten personell zu trennen. Leider hat es der Gesetzgeber in diesem Zusammenhang versäumt, für die Trennung eine europarechtskonforme Übergangsvorschrift vorzusehen. Da sich die Gremien von BR, Deutschlandradio, SR, WDR und ZDF aus Gründen der Wirtschaftlichkeit und Unabhängigkeit zusammengetan haben, um eine gemeinsame Aufsicht zu ernennen, lege ich mein Amt als Rundfunkdatenschutzbeauftragte hiermit rückwirkend vorzeitig zum 31. Dezember 2018 nieder.

Danken möchte ich der Justiziarin und stellvertretenden Intendantin, Eva-Maria Michel, die in Zeiten der Strukturreform immer ein offenes Ohr für mich hatte; meinem Ansprechpartner in Sachen Datenschutz im Justiziariat, Roland Boysen; Norbert Gust, IT-Sicherheitsbeauftragter, und Peter Ladwig, Gruppenleiter Netze und Security, die mich in Informationssicherheitsfragen stets hervorragend unterstützt haben; sowie den Mitgliedern des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) für die kollegiale Zusammenarbeit. Besonders danken möchte ich meiner Assistentin Petra Baumann sowie meiner studentischen Hilfskraft Benita Brüggenjürgen, die mich bei der Erstellung des Tätigkeitsberichts tatkräftig unterstützt haben sowie meinem Stellvertreter, Günter Grießbach, für seinen Einsatz im Rahmen meiner mutterschutzbedingten Abwesenheit.

1.2. …wird Rundfunkdatenschutzbeauftragte

Meine Aufgaben und Befugnisse als Aufsicht ergeben sich aus § 51 WDR-Gesetz in Verbindung mit Artikel 57 und 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung; im Folgenden kurz: DSGVO). Ich nehme auch die Aufgaben der Datenschutzbeauftragten nach Artikel 39 DSGVO wahr. Als Aufsichtsbehörde überwache ich die Einhaltung der Datenschutzvorschriften bei der gesamten Tätigkeit des WDR und seit dem 25. Mai 2018 auch seiner Beteiligungsunternehmen.

Im Berichtszeitraum gab es keinen Anlass für förmliche Beanstandungen im Sinne von § 51 Absatz 2 WDR-Gesetz.

Seit dem 25. Mai haben sich durch das Anwendungserfordernis der Artikel 57 und 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679 die Aufgaben und Befugnisse jeder Datenschutz-Aufsicht stark erweitert. Jede Aufsichtsbehörde muss in ihrem Hoheitsgebiet die Anwendung der Verordnung durchsetzen und Untersuchungen durchführen. Dafür stehen ihr durch die Datenschutzgrundverordnung weitreichende Untersuchungs- und Abhilfebefugnisse zur Verfügung. Neu ist diesbezüglich neben dem Mittel der Warnung oder Verwarnung, die Befugnis zur Anweisung durch die Aufsichtsbehörde. Die Aufsichtsbehörde muss die Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten und die Verantwortlichen für ihre Pflichten aus der Verordnung sensibilisieren. Die Datenschutzgrundverordnung verpflichtet des Weiteren alle Aufsichtsbehörden zur Zusammenarbeit. Erste Gespräche mit Vertretern der staatlichen Datenschutzaufsichten haben bereits stattgefunden. Darauf gehe ich unter Ziffer 6.2 näher ein.

Zur besseren Lesbarkeit habe ich den folgenden Tätigkeitsbericht erstmals in Themenschwerpunkte untergliedert und hoffe, meiner Verpflichtung zur Sensibilisierung und Aufklärung der Öffentlichkeit so bestmöglich zu entsprechen.

Köln, im März 2019 Karin Wagner

2. WhatsApp, WDR und DSGVO

DSGVO: Continental verbietet WhatsApp auf Diensthandys

Nach einer ARD/ZDF-Onlinestudie[1] waren 2018 erstmals über 90 Prozent der Deutschen online. Ein deutlicher Zuwachs sei bei der Nutzung von Medien und Kommunikation via Internet zu verzeichnen. Die tägliche Nutzungszeit im Internet sei im Schnitt auf 196 Minuten (3:16 Stunden) gestiegen; 47 Minuten mehr als 2017. Bei den unter 30-Jährigen betrage sie sogar knapp sechs Stunden. Knapp die Hälfte dieser Zeit wird mit Individualkommunikation verbracht, die in vielen Fällen auf Chatdiensten wie WhatsApp basiert. Denn der beliebteste Messenger in Deutschland ist auch 2018 weiter WhatsApp.[2]

So ist es nicht verwunderlich, dass auch der WDR weiter auf WhatsApp setzt, um sein Publikum zu erreichen. Das gefällt Vielen nicht, wie das folgende Beschwerde-Beispiel zeigt:

»Sehr geehrte Damen und Herren,

ich finde es unerträglich, dass Sie ein Unternehmen fördern, das massiv gegen den Datenschutz verstößt.

Sowohl auf WDR 4 als auch auf 1LIVE, etc. wird man regelmäßig aufgefordert, per WhatsApp zu kommunizieren.

Warum bietet man nicht für datenschutzorientierte Hörer andere Kanäle wie Threema etc. an?

Ich freue mich, von Ihnen zu lesen.

Mit freundlichen Grüßen nach Köln
Never-used-Whatsapp«

Grundsätzlich bin ich als Datenschützerin nicht glücklich über den Einsatz von WhatsApp im Programm-Angebot des WDR. Meine Zuständigkeit beschränkt sich aber darauf, datenschutzrechtlich zu beaufsichtigen, dass der WDR sich datenschutzkonform verhält.

In meinem ersten Berichtsschwerpunkt möchte ich deshalb erklären, was Kern des datenschutzrechtlichen Problems im Zusammenhang mit WhatsApp ist und warum der WDR nach meiner Auffassung WhatsApp datenschutzkonform einsetzt. Die massenhafte Verbreitung eines datenschutzunfreundlichen Geschäftsmodells zu stoppen, wäre dagegen Aufgabe der für das Unternehmen WhatsApp zuständigen staatlichen Datenschutzaufsichten.

2.1. Das datenschutzrechtliche Problem

WhatsApp ermöglicht Kommunikation über das Internet vermeintlich ohne Kosten. Die Nutzung der App kostet kein Geld, das ist wahr, aber sie kostet den Nutzer zwangsläufig die Preisgabe seiner Kontaktdaten. Daten sind der neue Rohstoff, der nur deshalb noch so leicht zu heben ist, weil den meisten Menschen die Fantasie fehlt, was man mit ihren »ich-hab-doch-nichts-zu-verbergen-Daten« alles anfangen kann und was sie dementsprechend wert sind. Der WDR ist gemeinnützig, WhatsApp ist es nicht. Es sollte demnach jedem einleuchten, dass der Marktwert der Kontaktdaten immens hoch sein muss, wenn einer der Global Player darauf sein Geschäftsmodell aufbaut.

Bei Installation der App muss der User seine Erlaubnis erteilen, dass sein Adressbuch ausgelesen wird. Für WhatsApp-Kontakte ist dies unproblematisch. Sie sind damit einverstanden, dass ihre Daten an WhatsApp weitergegeben werden; sie haben diese Datenübermittlung ja selbst bereits bei Installation der App autorisiert. Trotz der großen Marktdurchdringung befinden sich in einem Adressbuch aber in den meisten Fällen auch Kontakte, die sich nicht freiwillig in den WhatsApp-Kosmos begeben haben und dies unter Umständen auch bewusst nicht wollen. Die App-Kommunikation würde auch ohne diese Datenübermittlung funktionieren. Dennoch lässt WhatsApp eine Installation

[1] http://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie-2018/ heruntergeladen am 08.03.2019 10:10 Uhr.

[2] https://www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-verwenden-Messenger.html abgerufen am 08.03.2019 um 11:11 Uhr.

nur zu, wenn ein Vollzugriff auf das Telefonbuch gestattet wird.

Mangels Einwilligung ist die Datenübermittlung dieser personenbezogenen Kontaktdaten damit datenschutzrechtlich unzulässig. WhatsApp schiebt den schwarzen Peter dem einzelnen Nutzer zu. Es wird verlangt, dass sie für die Rechtmäßigkeit der Daten-Übermittlung garantieren:

»Wir verlangen von jedem dieser Nutzer und Unternehmen, dass sie die rechtmäßigen Rechte besitzen, um deine Informationen zu erfassen, zu verwenden und zu teilen, bevor sie uns irgendwelche Informationen bereitstellen. [3]«

2.2. Die Lösung

Im Zusammenhang mit der WhatsApp-Nutzung dürfen demnach keine Nicht-WhatsApp-Kontakte in einem Adressbuch gespeichert werden. Daran hält sich der WDR.

Die Nutzung von WhatsApp auf Firmen-Smartphones ist aus vorgenannten Gründen grundsätzlich nicht erlaubt. Es gibt aber die Möglichkeit das Adressbuch in einer sogenannten Container-App auszuführen, die einen Zugriff auf Kontakte von außerhalb des Containers unterbindet.

Grundsätzlich verwendet der WDR den WhatsApp-Dienst nur entweder für Newsletter-Dienstleistungen als Ausgangskanal oder zur Kontaktaufnahme, die ein Eingehen von Fotos, Anregungen und Meinungsäußerungen seitens des Publikums ermöglicht. In beiden Fällen befinden sich die Nutzer bereits in der WhatsApp-Welt und es werden entsprechend keine Daten von Personen verarbeitet, die nicht selbst bereits den WhatsApp-AGB zugestimmt haben.

Und so sieht das dann zum Beispiel aus:

2.2.1. Newsletter Push-Funktion

»Messenger-Service von WDR aktuell

Infos kommen per WhatsApp

Was bringt der Tag? Was ist los in NRW und der Welt? Was passiert in den sozialen Netzwerken? Antworten darauf gibt WDR aktuell jetzt auch über WhatsApp.

Morgens gibt's den Ausblick auf die wichtigsten Themen des Tages, abends einen Nachrichtenrückblick: WDR aktuell informiert jetzt auch über den Messenger-Dienst WhatsApp. Und natürlich liefern wir auch zwischendurch wichtige Neuigkeiten, damit Sie stets auf dem Laufenden sind. Der Schwerpunkt liegt dabei auf Nordrhein-Westfalen.

Hier kostenlos abonnieren:

Willkommen beim WhatsApp Service des Westdeutschen Rundfunks! Geben Sie einfach hier Ihre Mobilnummer ein, auf »hinzufügen« klicken, dann bitte der Anleitung folgen.

Wichtig: Sie aktivieren den Dienst nur durch eine WhatsApp-Nachricht mit dem Inhalt »START« an uns (SMS oder E-Mail funktionieren nicht). Für die Abmeldung »Stop« schreiben.

Sollten Sie Probleme mit der Anmeldung haben, bitte kurze Info an whatsapp@wdr.de.

Hinweise zum Datenschutz

Wenn Sie WhatsApp auf Ihrem Mobilgerät installieren und nutzen, stimmen Sie den Allgemeinen Geschäftsbedingungen von WhatsApp zu, auf die der WDR keinen Einfluss hat. Diese beinhalten unter anderem, dass die WhatsApp Inc. Zugriff auf Telefonnummern und die auf dem Mobilgerät gespeicherten Kontakte erhält. Ebenso werden Daten auf Servern von WhatsApp Inc. gespeichert, die nicht dem europäischen Datenschutzrecht unterliegen.

Der WDR, hier WDR aktuell, haftet nicht für Schäden, die durch Ihre Nutzung der WhatsApp-Plattform entstehen.

Welche Daten werden vom WDR gespeichert und was passiert mit diesen Daten?

Der WDR arbeitet bei diesem Service mit dem österreichischen Dienstleister ATMS zusammen. Folgende Daten werden im ATMS-Rechenzentrum gespeichert:

- *Ihre Rufnummer, mit der Sie sich bei unserem WhatsApp-Dienst angemeldet haben.*

[3] https://www.whatsapp.com/legal?eea=1&lang=de abgerufen am 8.3.2019 um 13:37 Uhr.

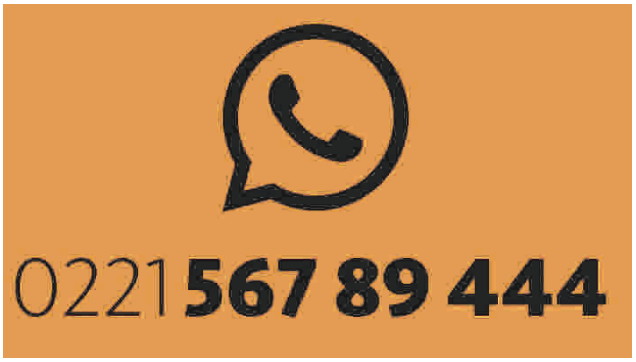
\ *Ihr Nutzername, den Sie sich bei WhatsApp gegeben haben. Abhängig von Ihrer Wahl kann dieser den Vor- bzw. Nachnamen beinhalten.*
\ *Nachrichten, die Sie dem WDR über WhatsApp senden.*

Wir verwenden diese Daten nur und ausschließlich für die WhatsApp-Kommunikation mit Ihnen sowie ggf. für telefonische Rückfragen im Rahmen von Programmaktionen des WDR. Wir bzw. ATMS geben diese Daten ohne Ihre ausdrückliche Zustimmung nicht an Dritte weiter.

Alle durch ATMS gespeicherten Daten werden in Europa verarbeitet und gehostet und unterliegen daher dem EU-Datenschutz. Nur autorisiertes Personal hat Zugang zum ATMS-Rechenzentrum.«

2.2.2. Kontaktaufnahme via WhatsApp

»



Schreiben Sie uns über WhatsApp

Ob Musikwunsch, nette Worte oder sonstiges Feedback - wir freuen uns immer. Schicken Sie uns Ihre Nachrichten, Fotos, Videos oder eine Sprachnachricht gerne auch über WhatsApp.

Sie erreichen uns bei WhatsApp unter der Nummer 0221 - 567 89 444. Bitte vergessen Sie nicht, uns Ihren Namen und Wohnort dazuzuschreiben.

Was passiert mit Ihren Nachrichten?

Mit dem Absenden erklären Sie sich einverstanden, dass der Inhalt Ihrer Nachricht (Audio, Video, Foto, Text) im Angebot von WDR 4 veröffentlicht wird. Der WDR darf die Inhalte der Nachrichten im Rahmen seiner Berichterstattung über WDR 4 in sämtlichen WDR-Formaten und auf sämtlichen Drittplattformen verwenden.

Datenschutz bei WhatsApp

Wenn Sie über den Instant-Messenger-Dienst WhatsApp Kontakt mit uns aufnehmen, übermitteln Sie uns damit automatisch Ihre Telefonnummer. Diese wird auf gesicherten mobilen Endgeräten des Westdeutschen Rundfunks gespeichert. Wir erstellen keine Userprofile und geben die Daten nicht an Dritte weiter, soweit dies nicht durch die allgemeinen Geschäftsbedingungen von WhatsApp bereits als Nutzungsbedingung festgelegt ist. Wir verwenden die Kontaktnummer bzw. Mobilnummer nur und ausschließlich für die WhatsApp-Kommunikation mit Ihnen sowie ggf. für telefonische Rückfragen im Rahmen von Programmaktionen des WDR bzw. von WDR 4.

Bitte beachten Sie, dass die Vertraulichkeit und Datensicherheit bei Instant-Messenger-Diensten wie WhatsApp nicht gewährleistet ist. Wenn Sie WhatsApp auf Ihrem Mobilgerät installieren und nutzen, stimmen Sie den Allgemeinen Geschäftsbedingungen von WhatsApp zu, auf die der WDR keinen Einfluss hat. Diese beinhalten unter anderem, dass Sie der WhatsApp Inc. Zugriff auf Ihre Telefonnummer und die auf Ihrem Mobilgerät gespeicherten Kontakte gewähren. Ebenso werden Daten auf Servern von WhatsApp Inc. gespeichert, die nicht dem europäischen Datenschutzrecht unterliegen.

Der WDR, hier WDR 4 , haftet nicht für Schäden, die durch Ihre Nutzung der entsprechenden Plattformen entstehen.«

3. Facebook, EuGH, gemeinsame Verantwortung

Und so wie die Daten von WhatsApp zu Facebook fließen, leite ich über zu meinen nächsten Schwerpunkt:

EuGH: Betreiber einer Facebook-Fanpage haftet gemeinsam mit Facebook für Verarbeitung personenbezogener Daten auf Fanpage

Ich habe dem WDR nicht empfohlen seine Fanpages offline zu stellen. Warum habe ich das nicht getan und welche Handlungsempfehlungen habe ich gegeben?

3.1. Die Vorabentscheidung des EuGH

Mit seinem Urteil in der Rechtssache C-210/16 hat der EuGH entschieden, dass der Betreiber einer Facebook-Fanpage gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage verantwortlich ist.

Diese Entscheidung erging auf eine Vorlage des Bundesverwaltungsgerichts in einem sogenannten Vorabentscheidungsersuchen. Das Bundesverwaltungsgericht hatte dem Gerichtshof sechs Fragen zur Vorabentscheidung vorgelegt. Die hier näher behandelten ersten beiden Fragen beziehen sich darauf, ob und inwieweit der Betreiber einer auf Facebook unterhaltenen Fanpage gemeinsam mit Facebook einen Beitrag zur Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher dieser Fanpage leistet und somit ebenfalls als „für die Verarbeitung Verantwortlicher“ angesehen werden kann. Sie finden einen Auszug des Urteils in Bezug auf diese beiden Fragen, abgedruckt im Anhang unter 10.1.

Unstreitig entscheidet in erster Linie Facebook über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen, die die auf Facebook unterhaltenen Fanpages besuchen. Ziel des europäischen Datenschutzrechts ist es laut Gerichtshof ein hohes Niveau des Schutzes der Grundfreiheiten und Grundrechte natürlicher Personen, insbesondere ihrer Privatsphäre, bei der Verarbeitung personenbezogener Daten zu gewährleisten. Diesem Ziel entsprechend ist der Begriff des „für die Verarbeitung Verantwortlichen“ nach Ansicht des EuGH weit definiert.

Verantwortlich im Sinne der DSGVO ist, wer nach Artikel 4 Ziffer 7 über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[4] Hierzu urteilt der EuGH in Randnummern 38 f.:

»38 Zwar werden die von Facebook erstellten Besucherstatistiken ausschließlich in anonymisierter Form an den Betreiber der Fanpage übermittelt, jedoch beruht die Erstellung dieser Statistiken auf der vorhergehenden Erhebung – durch die von Facebook auf dem Computer oder jedem anderen Gerät der Personen, die diese Seite besucht haben, gesetzten Cookies – und der Verarbeitung der personenbezogenen Daten dieser Besucher für diese statistischen ***Zwecke****. Die Richtlinie 95/46 verlangt jedenfalls nicht, dass bei einer gemeinsamen Verantwortlichkeit mehrerer Betreiber für dieselbe Verarbeitung jeder Zugang zu den betreffenden personenbezogenen Daten hat.*

39 Unter diesen Umständen ist festzustellen, dass der Betreiber einer auf Facebook unterhaltenen Fanpage ***durch die von ihm vorgenommene Parametrierung*** *u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten* ***an der Entscheidung über*** *die* ***Zwecke und Mittel der Verarbeitung*** *der* ***personenbezogenen Daten*** *der Besucher seiner Fanpage* ***beteiligt*** *ist. Daher ist der Betreiber im vorliegenden Fall als in der*

[4] Exkurs Verhältnis zum Personalrat: Durch die DSGVO wurde auch die datenschutzrechtliche Verantwortung von Personalräten hinterfragt. Für den WDR bleibt es nach meinem Verständnis bei den althergebrachten Grundsätzen, die meines Erachtens mit der geltenden Gesetzeslage, gerade im Hinblick auf den unveränderten § 65 Absatz 4 Landespersonalvertretungsgesetz NRW vereinbar sind: *»Die Einhaltung des Datenschutzes obliegt dem Personalrat. Der Dienststelle sind getroffene Maßnahmen mitzuteilen.«*

Union gemeinsam mit Facebook Ireland für diese Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 einzustufen.«

Nach Feststellung des EuGH ist der Fanpage-Betreiber also durch die von ihm vorgenommene Parametrierung an der Entscheidung über Zwecke und Mittel der Verarbeitung personenbezogener Daten beteiligt. Diese Feststellung geht nach meinem Kenntnisstand von einer nicht aktuellen Tatsachenlage aus. Fanpage-Betreiber erhalten anonymisierte Daten, auf deren Zusammenstellung sie keinen Einfluss nehmen können.

Der EuGH ist keine Tatsacheninstanz. Er entscheidet im Rahmen eines Vorabentscheidungsverfahren nach Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union über die Auslegung europäischen Rechts, hier der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Abzuwarten bleibt, wie das Bundesverwaltungsgericht diese Entscheidung umsetzen wird und den Begriff des Verantwortlichen in Bezug auf die fehlende Parametrierung auslegt.

3.2. Seiten-Insights-Ergänzung

Am 5. September 2018 reagierte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit einem Beschluss.[5] Ohne Vereinbarung nach Art. 26 DSGVO sei laut Beschluss der Betrieb einer Facebook-Fanpage rechtswidrig.

An dieser Stelle möchte ich klarstellen, dass dieser Beschluss weder mit mir oder den anderen Rundfunkdatenschutzbeauftragten noch mit den übrigen europäischen Aufsichten abgestimmt war. Damit konnte er für den WDR zu keiner Zeit irgendeine Bindungswirkung entfalten.

Auch wenn ich mich, wie meine Rundfunkdatenschutzkollegen/innen, der Rechtsauffassung der staatlichen Kolleginnen und Kollegen in dieser absoluten Form nicht anschließen konnte, ist die Forderung der DSK im Kern aufgrund der Entscheidung des EuGH konsequent, da die DSGVO bei einer gemeinsamen Verantwortlichkeit eine Vereinbarung zwischen den Beteiligten fordert, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Nach Art. 26 Absatz 1 Satz 2 ff. DSGVO legen gemeinsam Verantwortliche

»in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß der 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. 3In 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.«

In Europa ist sie nicht neu, die gemeinsame Verantwortlichkeit im Sinne von Artikel 26 DSGVO. Für den deutschen Datenschutz, der bisher nur klar abgegrenzte Verantwortlichkeiten kannte, wirft sie Fragen auf.

Tatsächlich stellte Facebook am 12. September 2018 eine sogenannte „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ zum Abruf bereit.[6] Diese müsste den Anforderungen einer Vereinbarung im Sinne von Artikel 26 Absatz 1 Satz 2 DS GVO genügen.

Die Ergänzung legt fest, dass Facebook Ireland und der Fanpage-Betreiber gemeinsam Verantwortliche für die Verarbeitung von Insights-Daten sind. Facebook Ireland übernimmt die primäre Verantwortung gemäß DSGVO für die Verarbeitung von Insights-Daten und sämtliche Pflichten aus der DSGVO im Hinblick auf die Verarbeitung von Insights-Daten. Facebook Ireland stellt das

[5] https://www.datenschutzzentrum.de/uploads/facebook/20180905-DSK-Facebook-Fanpages.pdf abgerufen am 12.03.19 um 14:58 Uhr.

[6] https://de-de.facebook.com/legal/terms/page_controller_addendum abgerufen am 12.03.19 um 15:22 Uhr; abgedruckt im Anhang unter 10.2.

Wesentliche der Seiten-Insights-Ergänzung den betroffenen Personen zur Verfügung und erfüllt damit die Informationspflicht aus Artikel 26 Abs. 2 S. 2 DSGVO.

Einige Pflichten werden dem Fanpage-Betreiber auferlegt. Für praktisch nicht umsetzbar halte ich in diesem Zusammenhang, die Festlegung, dass der Fanpage-Betreiber sicherstellen soll, dass die Verarbeitung von Insights-Daten auf eine entsprechende Rechtsgrundlage der DSGVO gestützt werden kann. Die Rechtsgrundlagen von Artikel 6 DSGVO beziehen sich sämtlich auf die Verarbeitung personenbezogener Daten. Der Fanpage-Betreiber verarbeitet aber keine personenbezogenen Daten, sondern erhält, wie der EuGH selbst richtig feststellt nur anonymisierte Daten.

Bei allem Verständnis für eine teleologisch weite Auslegung des Begriffs der Verantwortlichkeit zum Schutz von hinter den personenbezogenen Daten stehenden Personen, scheint sich der europäische Datenschutz in diesem Zusammenhang erneut vor einem Kampf mit Goliath zu drücken. Insoweit bleibt es mir nur, gespannt auf die Konkretisierung durch das Bundesverwaltungsgericht zu schauen.

3.3. Angepasste Datenschutzerklärung des WDR

Aufgrund der unklaren Rechtslage habe ich dem WDR eine Anpassung seiner Datenschutzerklärungen empfohlen:

»Der Datenschutz bei Onlinepräsenzen des WDR in sozialen Medien wie Facebook, Twitter, Youtube und Instagram

Der WDR und seine verschiedenen Redaktionen sind innerhalb sozialer Netzwerke und Plattformen aktiv und präsent, um dort mit Interessenten und Nutzern zu kommunizieren und sie über weitere Angebote informieren zu können. Wie der Europäische Gerichtshof (Urt. v. 05.06.2018 – C-210/16) festgestellt hat, sind bei diesen sogenannten Fanpages neben den Portalinhabern (hier Facebook) auch die Betreiber der Seiten für die Datenverarbeitung mit verantwortlich.

Deshalb informiert der WDR hier über die Datenverarbeitung, soweit wir diese kennen und beeinflussen können.

Art und Zweck der Datenverarbeitung

Zur Auswertung des Nutzerverhaltens erhebt Facebook personenbezogene Daten. Einen Teil dieser Daten stellt Facebook den Betreibern von Fanpages in anonymisierter Form zur Verfügung. Als Betreiber dieser Fanpages erhält auch der WDR anonymisierte Statistik-Daten von Facebook oder über einen vom WDR beauftragten Dienstleister. Über diese Daten lassen sich keine Rückschlüsse auf die jeweilige Person ziehen. Diese Daten werden nur für die Analyse des Nutzerverhaltens verwendet, damit der WDR seine Angebote besser auf die Bedürfnisse und Interessen seines Publikums ausrichten kann. Der WDR kann dabei lediglich die Kategorien der Daten und Personen vorgeben, nach denen Facebook seine Datensammlung auswertet und in Form anonymisierter Statistiken zur Verfügung stellt. Welche Daten Facebook insgesamt sammelt und zu welchen Zwecken Facebook sie verarbeitet, ist dem WDR nicht bekannt. Wir bitten um Verständnis, dass wir Sie nur so weit informieren können, wie unser Wissen über die Datenverarbeitung und unser Einfluss auf die Datenverarbeitung reichen.

Der WDR weist aber darauf hin, dass die Betreiber der Plattformen meist amerikanische Firmen sind und somit ihre Daten auch außerhalb der Europäischen Union verarbeitet werden können. Hierdurch können sich Risiken ergeben, weil so z.B. die Durchsetzung der Rechte der Nutzerinnen und Nutzer erschwert werden könnte. Im Hinblick auf die US-Anbieter, die unter dem Privacy-Shield (Eine Datenschutzregelung zwischen der Europäischen Union und den USA) zertifiziert sind, weist der WDR darauf hin, dass diese sich damit verpflichten, die Datenschutzstandards der EU einzuhalten. Näheres dazu regeln die Datenschutzerklärungen der einzelnen Anbieter.

Facebook:

Firmensitz: Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland

\ *Datenschutzerklärung: https://www.facebook.com/about/privacy/*

\ *Opt-Out: https://www.facebook.com/settings?tab=ads und http://www.youronlinechoices.com*

\ *Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC&status=Active*

Google / YouTube

Firmensitz: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

\ *Datenschutzerklärung: https://policies.google.com/privacy*

\ *Opt-Out: https://adssettings.google.com/authenticated*

\ *Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active.*

Instagram

Firmensitz: Instagram Inc., 1601 Willow Road, Menlo Park, CA, 94025, USA

\ *Datenschutzerklärung: https://help.instagram.com/519522125107875?helpref=page_content*

\ *Opt-Out: Instagram bietet keine eigene Opt-Out Funktion, verweist aber auf die Funktionen der einzelnen Werbepartener-Agenturen wie Network Advertising Initiative unter http://www.networkadvertising.org/managing/opt_out.asp, die Digital Advertising Alliance unter http://www.aboutads.info/ oder die European Digital Advertising Alliance unter http://youronlinechoices.eu/http://instagram.com/about/legal/privacy/*

\ *Privacy Shield: Instagram hat sich nicht für das Amerikanisch-Europäische Datenschutzschild zertifizieren lassen.*

Twitter

Firmensitz: Twitter Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, USA

\ *Datenschutzerklärung: https://twitter.com/de/privacy*

\ *Opt-Out: https://twitter.com/personalization*

\ *Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt000000000TORzAAO&status=Active*

WhatsApp

Firmensitz: WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland

\ *Datenschutzerklärung: https://www.whatsapp.com/legal/?lang=de#privacy-policy*

\ *Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt000000000TSnwAAG&status=Active«*

4. Office 365, Niederlande und der CLOUD Act

Eine Frage, deren Beantwortung einen weiteren Schwerpunkt meiner Tätigkeit im Berichtszeitraum ausmachte: Kann Office 365 in einer öffentlich-rechtlichen Rundfunkanstalt datenschutzkonform eingesetzt werden? Um es vorwegzunehmen, eine abschließende Antwort auf diese Frage habe ich noch nicht.

Untersuchung: Microsoft Office sammelt Daten und verstößt gegen die DSGVO

Microsoft wirbt mit dem Motto:

»Die einfachste Art der Zusammenarbeit«.

Es handelt sich um das altbekannte Büropaket mit Word, Excel, Powerpoint und Outlook, das Microsoft als Mietmodell in die Cloud verlegt und mit Kollaborations-Features, wie Teams ergänzt.

Zur möglichen Einführung von Office 365 hat es eine Stellungnahme des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) vom 03. November 2017 gegeben, die ich als Anlage diesem Bericht beifüge und der ich mich grundsätzlich anschließe (siehe 10.3).

4.1. Cloud Computing

Auf das Thema Cloud bin ich in meinem letzten Bericht bereits ausführlich eingegangen.

Einfach ausgedrückt handelt es sich bei der Inanspruchnahme eines Cloud-Dienstleisters um das Outsourcen von Soft- oder Hardware in das Internet. Durch die weltweite Vernetzung benötigen Unternehmen immer mehr Leistung (Rechenleistung, Speicher, Performance). Man mietet Server-Kapazität im Netz. Bei diesem Mietmodell ging es anfangs schlicht darum Spitzen des eigenen Unternehmens dadurch abzufangen, dass man den Leerlauf fremder Server-Kapazitäten nutzt. Letztendlich also eine Art Server-Sharing. Wie auch bei anderen Share-Modellen machen Kostenersparnis und hohe Flexibilität den Dienst attraktiv. Ein weiterer praktischer Pluspunkt ist die Zugriffsmöglichkeit auf Daten von überall, solange eine stabile Internet-Verbindung besteht.

Bei Office 365 handelt es sich um eine cloudbasierte Softwarelösung. Nutzungsabhängig zahlt der Nutzer dem Anbieter einen Mietzins für den Dienst. Die gesamte zugrunde liegende Infrastruktur, Middleware und Software sowie die Daten befinden sich im Datencenter des Dienstanbieters. Der Dienstanbieter verwaltet die Hardware und die Software und stellt bei Abschluss eines entsprechenden Servicevertrags Verfügbarkeit, Integrität und Vertraulichkeit sicher. Der Nutzer muss sich infolgedessen nicht um Wartung der Programme oder Administration eines Servers kümmern. Aktualisierungen werden automatisch installiert. Die hauseigene IT wird potentiell entlastet.

Problematisch an solchen Cloud-Lösungen ist, dass die Leistungen so stark standardisiert angeboten werden, dass Verträge in wesentlichen Teilen nicht verhandelbar sind. Anbieter erzeugen sogenannte Lock-in-Effekte durch hohe Wechselkosten und praktische Wechselbarrieren. Die datenschutzrechtliche Verantwortung bleibt beim Auftraggeber, obwohl dieser die Kontrolle weitestgehend abgibt. *»Der Auftraggeber hat die Zulässigkeit der Datenverarbeitung zu prüfen, die Erfüllung der Nutzerrechte zu gewährleisten und mögliche Haftungsrisiken zu tragen. Es gibt detaillierte gesetzliche Vorgaben, welche Rechte, Pflichten und Maßnahmen in diesem Fall durch eine gesonderte schriftliche Vereinbarung zwischen dem Auftraggeber und dem Dienstleister zu treffen sind. Ganz wesentlich ist dabei die Datensicherheit: Das Schutzniveau für die Daten muss mindestens dem Schutzniveau bei Abwicklung im eigenen Unternehmen entsprechen.*[7]*«*

Bei Dienstleistungen im Zusammenhang mit Office 365 verarbeitet Microsoft nach eigener Aussage personenbezogene Daten im Auftrag seiner Kunden. Entsprechend müsste sich die Auftragsverarbeitung nach

[7] Aus LEITLINIEN ZUM DATENSCHUTZ IN DEN TELEMEDIEN- UND SOCIAL-MEDIA-ANGEBOTEN DER RUNDFUNKANSTALTEN des AK DSB; abgedruckt als Social-Media-Leitfaden im Anhang meines letzten Berichts.

Artikel 28 DSGVO richten. Auf das Thema Auftragsdatenverarbeitung bin ich bereits in meinem letzten Bericht eingegangen.

Durch die DSGVO wurde aus Auftragsdatenverarbeitung Auftragsverarbeitung. Artikel 28 DSGVO orientiert sich stark an den bisherigen nationalen Vorschriften (für den WDR war das § 11 DSG NRW alte Fassung). Der Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio hat ein Muster für eine Auftragsverarbeitungsvereinbarung erarbeitet (siehe Anlage 10.4), auf das sich Microsoft erwartungsgemäß nicht einlässt. Seit dem 25. Mai 2018 neu vergebene Aufträge basieren grundsätzlich auf dem Muster.

Exkurs zum Thema Wartung: Unter Datenschutz-Experten hat zu Diskussionen geführt, dass die DSGVO anders als die bisherigen Regelungen zum Thema Wartung schweigt. Teile der Literatur haben daraus geschlossen, dass es sich bei Wartungsaufträgen deshalb nicht um Auftragsverarbeitungen im Sinne der DSGVO handele. Da die Vertreter dieser Ansicht stattdessen auf alternative Vertraulichkeitsvereinbarung setzen, bleibt der Streit wohl eher akademisch. Für NRW hat der Landesgesetzgeber durch § 52 Absatz 2 DSG NRW klargestellt, dass Artikel 28 Absatz 1 bis 4, 9 und 10, sowie Artikel 29 DSGVO im Zusammenhang mit Wartung entsprechend anzuwenden sind.

4.2. Online Service Terms

Microsoft versucht den Anforderungen von Artikel 28 DSGVO durch seine sogenannten Online Service Terms (OST)[8] gerecht zu werden. Meines Erachtens erfüllt die aktuelle Version dieser Service Terms die Anforderungen von Artikel 28 DSGVO nicht.

Problematisch ist in meinen Augen insbesondere, dass sich Microsoft weigert, den Zweck der Verarbeitung entsprechend Art. 28 Absatz 3 Satz 1 DSGVO einzugrenzen. In den OST heißt es, Kundendaten würden dazu genutzt, dem Kunden Onlinedienste einschließlich der mit der Bereitstellung dieser Dienste kompatiblen Zwecke zur Verfügung zu stellen. Das widerspricht dem Konstrukt der Auftragsverarbeitung eklatant. Außerdem ist nicht abzusehen, was Microsoft für „mit dem Vertragszweck kompatibel“ hält. Streng genommen bestimmt Microsoft dadurch Zwecke und Mittel der Verarbeitung und wäre entsprechend datenschutzrechtlich nicht Auftragsverarbeiter, sondern Verantwortlicher. Diese Verantwortung lehnt Microsoft aber ab.

Datenschutzrechtlich problematisch ist meines Erachtens weiter, dass aus den OST nicht konkret hervorgeht, wann welche Daten zu welchem Zweck den europäischen Rechtsraum in welches Drittland verlassen. Grundsätzlich erlauben die OST Microsoft nach meinem Verständnis, Kundendaten in jedem Land zu verarbeiten in dem Microsoft, von Microsoft kontrollierte Tochtergesellschaften und verbundene Unternehmen oder ihre Unterauftragsverarbeiter tätig sind. Bestimmte geografische Gebiete, wie die EU, sichert Microsoft nur für nicht näher definierte „ruhende Daten“ und bestimmte Dienste zu.

In Bezug auf die technisch-organisatorischen Maßnahmen soll der Auftraggeber die Verantwortung dafür übernehmen, dass die von Microsoft ergriffenen Maßnahmen den Datenschutzvorschriften entsprechen. Artikel 28 Absatz 1, Absatz 3 Buchstabe c) DSGVO sehen diese Pflicht interessengerecht in der Sphäre des Auftragsverarbeiters. Dem Auftraggeber obliegt allein eine Überwachungspflicht.

4.3. Microsoft und die Niederlande

Laut einer im Auftrag des niederländischen Justizministeriums durchgeführten Untersuchung des Software-Pakets »Microsoft Office ProPlus«, die im November 2018 veröffentlicht wurde, *»sammelt und speichert* Microsoft *personenbezogene Daten über das Verhalten einzelner Personen in großem Umfang ohne jegliche öffentliche Dokumentation.«*[9]

Folgende Zitate aus der Untersuchung sprechen für sich:

»Microsoft sammelt systematisch und in großem Umfang Daten über die individuelle Nutzung von Word, Excel, PowerPoint und Outlook. Und das heimlich, ohne die Leute zu informieren. Microsoft bietet keine Wahl in Bezug auf die Datenmenge, die Möglichkeit, die Sammlung auszuschalten, oder die Möglichkeit, zu sehen, welche Daten gesammelt werden, da der Datenstrom verschlüsselt ist. Ähnlich wie bei Windows 10 hat Microsoft in die Office-Software eine separate Software

[8] https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx abgerufen am 19. März 2019.
[9] DPIA-Prüfbericht von Privacy Company auf Deutsch heruntergeladen von https://www.privacycompany.de/datenschutz-folgenabschatzung-zeigt-risiken-bei-microsoft-office-proplus-enterprise/ am 14.03.2019 um 16:59 Uhr.

integriert, die regelmäßig Telemetriedaten an ihre eigenen Server in den USA sendet.«

»Microsoft bestimmt den Zweck der Verarbeitung der Diagnosedaten in der Office-Software und die Aufbewahrungsfrist der Daten (30 Tage bis zu 18 Monate, wenn Microsoft es für notwendig hält, sogar länger): […] 4. Produktentwicklung (neue Funktionen hinzuzufügen)

5. Produktinnovation (Business Intelligence, Entwicklung neuer Dienstleistungen)

6. Allgemeine Schlussfolgerungen aus der Langzeitanalyse, Unterstützung des maschinellen Lernens

7. Gezielte Empfehlungen auf dem Bildschirm für den Benutzer anzeigen

8. Ziele, die Microsoft für kompatibel mit diesen 7 Zielen hält.«

»Es verbleiben jedoch 6 hohe Risiken für die betroffenen Personen:

1. Die rechtswidrige Speicherung sensibler, klassifizierter oder spezieller Datenkategorien, sowohl in Metadaten als auch z.B. in Betreffzeilen von E-Mails.

2. Die falsche Qualifikation von Microsoft als Auftragsverarbeiter und nicht als Mitverantwortlicher im Sinne von Artikel 26 der DSGVO.

3. Unzureichende Kontrolle über untergeordnete Auftragsverarbeiter und faktische Auftragsverarbeitung.

4. Die fehlende Zweckbindung, sowohl für die Verarbeitung historisch gesammelter Diagnosedaten als auch für die Möglichkeit, neue Arten von Ereignissen dynamisch hinzuzufügen.

5. Die Übermittlung von (allen Arten von) Diagnosedaten außerhalb des Europäischen Wirtschaftsraums, während die aktuelle Rechtsgrundlage für Office ProPlus das Privacy Shield ist und die Gültigkeit dieser Vereinbarung Gegenstand eines Verfahrens vor dem Europäischen Gerichtshof ist.

6. Die unbestimmte Aufbewahrungsdauer von Diagnosedaten und das Fehlen eines Tools zum Löschen historischer Diagnosedaten.«

»Was die Verträge und die Übermittlung personenbezogener Daten an die USA betrifft, so muss eine europäische Lösung gefunden werden. SLM Rijk und Microsoft werden sich in den kommenden Monaten weiterhin eng abstimmen. In der Zwischenzeit führt Privacy Company eine weitere Untersuchung des Inhalts der Telemetriedaten durch.«

Es bleibt also spannend.

4.4. Trump und sein CLOUD Act

Am 23. März 2018 stellte die Trump-Regierung den Datenzugriff auf US-ausländische Server durch ein neues US-Gesetz, den CLOUD Act, sicher.

Microsoft hatte sich einer richterlichen Anordnung auf Datenherausgabe widersetzt, weil sich die Daten nicht auf Servern in den USA, sondern in Irland befanden. Am 17. April 2018 erklärte das höchste US-amerikanische Gericht, den Rechtsstreit für erledigt. Grund dafür ist der CLOUD Act. CLOUD steht für *»Clarifying Lawful Overseas Use of Data Act«.* Der CLOUD Act verpflichtet US-Unternehmen zur Datenherausgabe, egal ob der Speicherort sich im US-Inland befindet oder nicht und unabhängig davon, ob Gesetze am Speicherort dies verbieten.

Diese Offenlegung von Kundendaten gegenüber Strafverfolgungsbehörden nach dem Cloud Act verstößt klar gegen Artikel 48 DSGVO. Nach Artikel 48 DSGVO dürfen Daten eines Auftragsverarbeiters nur dann aufgrund der Entscheidung eines Gerichts oder einer Behörde im EU-Ausland an das Drittland übermittelt werden, wenn eine internationale Übereinkunft, wie etwa ein Rechtshilfeabkommen dies vorsieht.

4.5. Exkurs: Alexa und Co

Immer wieder werde ich mit Nutzungswünschen in Bezug auf sprachgesteuerte Personal Assistants konfrontiert. Für Testzwecke halte ich eine Nutzung für möglich, wenn berücksichtigt wird, dass sobald der Sprachassistent aktiviert ist, nicht ausgeschlossen werden kann, dass jeglicher Audiomitschnitt des Aufzeichnungsumfelds auf Server in die USA übermittelt und dort auf unbestimmte Zeit gespeichert wird. Der Sprachassistent darf deshalb ausschließlich in Hörweite von informierten Freiwilligen genutzt werden. Außerhalb vom Testbetrieb muss der Sprachassistent ausgeschaltet werden, da die Vorgabe einer informierten Freiwilligkeit aller von dieser Technik Betroffenen sonst nicht gewährleistet werden kann. Kurz:

\ Echo wird nur zu expliziten Testeinsätzen physisch eingeschaltet und ansonsten abgeschaltet und vom Netz getrennt.
\ Alle im Raum befindlichen Personen werden über jeden Einsatz informiert.
\ Während Testeinsätzen werden keine Telefonate geführt.
\ Vorab Versand einer Info-Mail an Mitarbeiter.

5. Cybersicherheit und Datenschutz

Gruppe »Sandworm«: WDR und ZDF von russischen Hackern angegriffen

Diese Schlagzeile sorgte Anfang Juni 2018 für große Aufmerksamkeit in weiten Kreisen - und müdes Gähnen bei vielen anderen. Dem »Spiegel« zufolge seien die IT-Netzwerke auch des WDR Anfang Juni Ziel einer Kampagne der russischen Hackergruppe Sandworm gewesen. Das Magazin berief sich auf Informationen aus Sicherheitskreisen.

Das ZDF bestätigte den Angriff. Weniger als zehn Rechner seien betroffen gewesen, keine Daten seien abgeflossen. Der WDR hat sich aus »sicherheitstechnischen Gründen« nicht geäußert.

Sandworm soll eine Hackergruppe des russischen Militärgeheimdienstes sein, die auch für Angriffe gegen die NATO, westliche Regierungsstellen, Telekommunikationsunternehmen und akademische Einrichtungen verantwortlich sein soll.

5.1. Was ist Cybersicherheit

Es wird Zeit, das Thema Cybersicherheit aus der Nerd-Ecke zu befreien und klarzustellen: Cybersicherheit geht uns alle an! Die Einschläge kommen näher und die IT allein kann heutzutage nichts mehr ausrichten. Ein achtsamer Umgang mit eingehenden Mails ist das A und O.

Aus diesem Grund möchte ich diesem Thema diesen weiteren Schwerpunkt meines Berichts widmen. Datenschutz ist ohne IT-Sicherheit heute nicht mehr denkbar. Datenschutz ist spätestens seit Wirksamwerden der DSGVO eine Querschnittsmaterie aus Recht, Technik und betriebswirtschaftlichem Know How.

Cybersicherheit befasst sich mit dem Schutz von Technik. Es geht um die Sicherheit von Computern, Servern, Netzwerken, mobilen Endgeräten und elektronischen Daten. Dieser Schutz wird erreicht durch Sicherheitssysteme, Prozessdefinitionen, auch durch den physischen Schutz von Gebäuden und Serverräumen; kurz gesagt durch im Datenschutzrecht als technisch-organisatorische Maßnahmen bekannten Schutzmechanismen.

Schutzobjekt des Datenschutzes ist der hinter den Daten stehende Mensch. Schnittmenge beider Aufgabengebiete ist damit der Schutz personenbezogener elektronischer Daten. Im Zeitalter des digitalen Wandels, wo die Zahl personenbeziehbarer IP-Adresse stetig steigt und durch Big Data Analytics selbst dort ein Personenbezug herstellbar ist, wo man es zunächst nicht vermutet, hat sich das Anwendungsgebiet des Datenschutzes immens vergrößert.

Personenbezogene elektronische Daten sind der Rohstoff unserer Zeit. Der diesbezügliche Internet-Schwarzmarkt ist international organisiert und mittlerweile lukrativer als Drogenhandel.[10]

5.2. Der »Promi-Hack«

Im Sommer 2017 fand das Bundeskriminalamt 500 Millionen ausgespähte Zugangsdaten. Wenn ein Passwort einmal in kriminellen Kreisen bekannt ist, wird es auch genutzt. So wurde ich im September 2018 informiert, dass Erpresser die damals geleakten Passworte nutzten. Wer damals sein Passwort für den korrumpierten Zugang und alle anderen zuordenbaren Accounts geändert hatte, konnte sich entspannen. Dass dies aber nicht in jedem Fall geschehen ist, machte ein Vorfall Ende 2018 deutlich.

Diverse Medien berichteten über *das größte Daten-Leck in der deutschen Geschichte*. *Handynummern, E-Mail-Adressen, private Fotos von knapp 1 000 Politikern, Prominenten und Journalisten* seien Opfer des *riesigen Hacker-Angriffs*. Hatte der Cyber-War im Gewand eines Twitter-Adventkalenders begonnen?

Bei nüchterner Herangehensweise muss man sagen, dass es sich bei dem Sachverhalt hinter den aufgeregten Schlagzeilen vermutlich nur um eine breit ange-

[10] https://www.divsi.de/cybercrime-profitabler-als-drogenhandel/ abgerufen am 27. März 2019 um 12:02 Uhr.

legte Internet-Recherche in Kombination mit vielzähligen Einbrüchen in private Kennungen gehandelt hat. Unternehmensnetze waren nicht betroffen. Es dürfte sich in einigen Fällen um eine Art Kettenreaktion gehandelt haben. Wenn ein korrumpierter Account beispielsweise Listen über Mailadressen oder Telefonnummern vieler weiterer interessanter Personen enthält und man diese Informationen sinnvoll mit bereits anderweitig im Internet bekannten Daten verknüpft, kommt man mit ein wenig Fleißarbeit an Unmengen von vertraulichen Daten.

Deshalb ist es so wichtig für verschiedene Zugänge auch verschiedene Passworte zu nutzen. Auch sollte man, wenn möglich keine Nutzernamen mit Bezug zum Realnamen wählen, weil dies die Verknüpfung für Hacker erleichtert.

5.3. Spear-Fishing

Früher wollten Angreifer möglichst schnell maximalen Schaden verursachen. Heute nehmen sich Angreifer zum Teil sehr viel Zeit und investieren viel Handarbeit und Mühe in ihre Angriffe. Warum tun sie das? Was ist das Ziel des Angriffs? Spionage? Der intendierte Erfolg scheint den Angreifern offenbar viel wert. Sie scheinen es darauf anzulegen, über einen möglichst langen Zeitraum unentdeckt im System zu bleiben. Oft ist sich ein Opfer aus diesem Grund seiner Opferrolle vielleicht gar nicht bewusst.

»Warum landet das nicht im Spam?« Mit meinem Bericht möchte ich Ihr Technikvertrauen erschüttern. Es war damals in den 00er Jahren, als man sich noch auf Virenscanner und Firewalls verlassen konnte. Was ist seitdem passiert? Gleich geblieben ist, dass auch heute noch Schadcodes hauptsächlich per Mail eingeschleust werden. Neu sind maßgeschneiderte Attacken, wie Sandworm.

Der WDR ist als Rundfunkanstalt eine sogenannte Kritische Infrastruktur. *»Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten. In Deutschland werden Medien und Kultur (Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke) den Kritischen Infrastrukturen zugeordnet.*[11]*«*

Der WDR genießt das Grundrecht der Rundfunkfreiheit, um seiner Rolle für die öffentliche Meinungsbildung gerecht werden zu können. Diese freie Meinungsbildung ist konstitutive Voraussetzung für eine funktionierende Demokratie. Als zweitgrößtes Medienunternehmen Europas ist der WDR damit selbstredend interessant für Angreifer.

Was könnten diese Angreifer wollen? Ein Schwarzbild, Propaganda oder Fake-News verbreiten, die Reichweite bekannter Journalisten nutzen oder die Reputation des WDR zerstören?

Eins sollte jedem klar sein. Wir müssen den Umstand akzeptieren, dass Angriffe stattfinden. Wir müssen uns auch klar darüber sein, dass Angreifer irgendwann Erfolg haben werden. Spear-Phishing ist nicht gänzlich zu verhindern. Auch wenn man seine Systeme aktuell hält und Mitarbeiter sensibilisiert, darf man aufgrund dieser Erkenntnis nichts ans Netz bringen, was Leib oder Leben Einzelner gefährden könnte.

5.4. Angriffserkennung

Wenn man Angriffe also als gegeben akzeptiert, muss man Angriffserkennungsmaßnahmen einleiten. Als anlassbezogene Stichproben-Analyse sind diese aus Datenschutzsicht unproblematisch. Eine erhöhte Alarmbereitschaft gab es im Zusammenhang mit dem Bundestag-Hack, bei besonderen Gefährdungslagen, wie kritischer Berichterstattung im Zusammenhang mit dem sogenannten Russland-Doping, bevorstehenden Wahlen und entsprechenden Warnungen aus Sicherheitskreisen. Aber ist es dann nicht vielleicht schon zu spät?

Der Markt reagiert. Angriffserkennungssysteme mit unterschiedlichen Eingriffsintensitäten kommen zum Einsatz. Diese untersuchen den gesamten Datenstrom auf Unregelmäßigkeiten und greifen dabei notwendigerweise auch auf personenbezogene Daten zu.

An diesem Punkt beginnt die Zwiespalt von Datenschutz und Datensicherheit. Personenbezogene Daten sollen sicher sein; verfügbar, integer und vertraulich. Aufgrund des Postulats der Datensparsamkeit, dürfen personenbezogene Daten nur in möglichst geringem Maß verarbeitet werden. Bei jeder prophylaktischen Angriffserkennungsmaßnahme handelt es sich streng genommen um eine Art von Vorratsdatenspeicherung. Wie passt das mit dem datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt zusammen, nach dem alles was

[11] Abgerufen von https://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html?lv2=4968594 am 18. März 2019.

nicht erlaubt, verboten ist. Die technische Entwicklung ist schnell, die Gesetze wie so häufig sehr vage.

Als Rechtsgrundlage für eine solche Datenverarbeitung im Sinne der DSGVO kommt keine rechtliche Verpflichtung in Betracht. Der WDR ist weder aus dem BSiG verpflichtet, entsprechende Schutzmaßnahmen zu treffen (siehe 5.5 am Ende), noch hilft die Ermächtigungsgrundlage Erwägungsgrund 49 der DSGVO, die nur Abwehrmaßnahmen gestattet, nicht jedoch Angriffserkennung.

Als gemeinnützige Anstalt des öffentlichen Rechts bleibt nur ein Rückgriff auf § 3 DSG NRW, soweit die Angriffserkennung für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist und eine Abwägung ergibt, dass keine überwiegenden schutzwürdigen Belange von Betroffenen entgegenstehen.

Meines Erachtens sollte dieses Spannungsverhältnis zwischen Datensicherheit und Datenschutz vom Gesetzgeber gelöst werden, um eine Abwägung der widerstreitenden Interessen zu vereinheitlichen und sie nicht dem Rechtsanwender zu überlassen.

5.5. Rechtslage zur Cybersicherheit

Krypto-Trojanern wie »WannaCry« fielen im Mai 2017 laut Europol 200 000 Opfer in 150 Ländern zum Opfer. Betroffen waren der US-amerikanischen Lieferdienst Fedex, die Deutsche Bahn, aber auch der britische Gesundheitsdienst NHS. Damit verursachte WannaCry nicht nur finanzielle Schäden in Millionenhöhe, sondern es standen auf einmal auch die Gesundheit und Menschenleben auf dem Spiel. Die NSA hatte von der Sicherheitslücke gewusst, diese aber nicht an das betroffene Unternehmen Microsoft weitergegeben.

Aus diesem Fehler wollte man lernen und es gab im Anschluss sowohl politische als auch Gesetzgebungsbestrebungen, die ein gemeinsames, transparentes Vorgehen anstrebten.

Am 10. Dezember 2018 erzielten das Europäische Parlament, der Rat und die Europäische Kommission insofern eine politische Einigung über den Rechtsakt zur Cybersicherheit, um eine bessere Bewältigung von Bedrohungen und Angriffen in diesem Bereich zu erzielen. Die EU hat hiermit das Mandat der „Agentur der Europäischen Union für Netz- und Informationssicherheit“ (ENISA) gestärkt. Der Rechtsakt zur Cybersicherheit schafft einen EU-Rahmen für die Cybersicherheitszertifizierung, der die Cybersicherheit von Online-Diensten und von Endgeräten für Verbraucher stärken soll.

Die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (sog. NIS-Richtlinie) trat bereits am 08. August in 2016 in Kraft und musste bis zum 09. Mai 2018 in deutsches Recht umgesetzt werden. Betreiber essentieller Dienste müssen hiernach zum einen bestimmte Sicherheitsstandards einführen und zum anderen Sicherheitsvorfälle melden. In Deutschland hielt man aufgrund des IT-Sicherheitsgesetzes vom 17. Juli 2015 und des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vom 14. August 2009 zuletzt geändert am 23. Juni 2017 nur wenige Anpassungen für erforderlich.

Der WDR fällt als Landesrundfunkanstalt nicht unter das BSIG, weil der Bundesgesetzgeber keine Gesetzgebungskompetenz für Landesrundfunkanstalten hat. Der nordrhein-westfälische Landesgesetzgeber ist bisher nicht tätig geworden. Das Saarland hat am 13. März 2019 ein umfassendes Informationssicherheitsgesetz erlassen und auch Bayern plant bis Ende 2020 ein umfassendes Maßnahmenpaket zur IT-Sicherheit. Die Gesetzesentwicklungen sind weiterhin zu beobachten.

6. Akkreditierung und staatliche Behörden

Champions-League-Spiel abgesagt: Sprengstoff-Anschlag auf Dortmunder Teambus - BVB-Profi verletzt

Das war die Schlagzeile im April 2017. Daraus leitete die Deutsche Fußballiga (DFL) eine höhere Sensibilität im Hinblick auf die Sicherheit bei Großveranstaltungen ab.

Vor diesem Hintergrund bat die DFL um Verständnis, dass vorsorglich auch private Anschrift und Geburtsdatum aller akkreditierten Personen im Rahmen eines Spiels der 1. oder 2. Bundesliga erfasst würden. Die Angabe dieser Informationen sei verbindlich und solle die zuständigen Sicherheitsbehörden in die Lage versetzen, im Falle einer konkreten Gefährdungslage etwaig gebotene und erforderliche Maßnahmen ergreifen zu können. Eine Weitergabe der Informationen an den jeweiligen Heim-Club solle auf Anfrage durch die DFL erfolgen.

6.1. Fehlende Rechtsgrundlage

Nach meiner Auffassung, die sich mit der der anderen Rundfunkdatenschutzbeauftragten deckt, fehlt für die Erhebung von Geburtsdaten und privater Anschrift von zu akkreditierenden Rundfunkmitarbeitern durch die DFL eine Rechtsgrundlage.

Die DFL stützt die Erhebung der Daten auf Artikel 6 Absatz 1 Buchstabe b) DSGVO und Artikel 6 Absatz1 Buchstabe e) DSGVO.

Nach Buchstabe b) wäre die Verarbeitung *rechtmäßig, wenn die Bedingung erfüllt ist: »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; «*

Nach Ansicht der DFL gehöre es zu den Nebenpflichten nach § 241 Absatz 2 BGB, der DFL als Lizenzgeberin die sichere Durchführung der Spiele und die Erfüllung gesetzlicher Verpflichtungen einschließlich der möglichen Anfragen von Sicherheitsbehörden zu ermöglichen.

Meiner Ansicht nach greift die genannte Rechtsgrundlage nicht. Es handelt sich dabei nicht um eine Rechtsgrundlage für die Sicherheitsbehörden, da die Rundfunkanstalten in diesem Verhältnis keinen Vertrag haben. Den Vertrag haben die Anstalten mit der DFL. Für die vertragsgemäße Akkreditierung sind laut DURCHFÜHRUNGSBESTIMMUNGEN zu den Medienrichtlinien, Spielzeit 2018/19[12] *»sämtliche Mitarbeiter und Beauftragte, die am Spieltag im Stadion arbeiten sollen, namentlich mit der jeweiligen Funktion sowie nach Möglichkeit einer mobilen Rufnummer zu benennen.«* Von Geburtsdatum und Privatanschrift als notwendige Information für eine Akkreditierung findet sich nichts. Im Übrigen wird kein Vertrag mit den Mitarbeitern geschlossen, sondern mit einer Rundfunkanstalt. Die privaten Daten der Mitarbeiter sind in diesem Zusammenhang demnach nicht Regelungsgegenstand von Buchstabe b).

Nach Buchstabe e) wäre die Verarbeitung *rechtmäßig, wenn die Bedingung erfüllt ist: »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;«* Nach Artikel 6 Absatz 3 DSGVO bedarf es einer gesetzlichen Grundlage für die Zuweisung der im öffentlichen Interesse liegenden Aufgabe oder der öffentlichen Gewalt:

»Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch Unionsrecht oder 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

[12] https://www.dfl.de/wp-content/uploads/sites/2/2018/11/Durchfuehrungsbestimmungen-2018-2019.pdf Seite 7 abgerufen am 15. März 2019 um 12:20 Uhr.

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.«

Die DFL hat im Verlauf weder eine unionsrechtliche noch eine mitgliedstaatliche Rechtsgrundlage vorgetragen.

6.2. Zusammenarbeit der Aufsichtsbehörden

Da die DFL immer wieder mit Nicht-Akkreditierung drohte und eine von der Gegenseite als Ausweg genannte Einwilligung der betreffenden Rundfunkmitarbeiter mangels Freiwilligkeit keine Alternative bot, wandten sich die Rundfunkdatenschutzbeauftragten zu Beginn der Saison 17/18 aufgrund des wachsenden Drucks der DFL und einzelner Fußballclubs an den hessischen Beauftragten für Datenschutz und Informationsfreiheit (HDBI). Als Aufsicht über die in Frankfurt ansässige DFL erhoffte sich der AKDSB ein Einschreiten von staatlicher Seite. Als Aufsicht über den öffentlich-rechtlichen Rundfunk konnte der AKDSB allein dafür sorgen, dass sich die Rundfunkmitarbeiter datenschutzkonform verhielten. Gegen den durch die DFL ausgeübten vertraglichen Zwang war der AKDSB machtlos. Die Zuständigkeit für die Verhinderung des angedrohten Datenschutzverstoßes lag in der Sphäre des HDBI.

Mit der Feststellung, dass der datenverarbeitende Dienstleister der DFL seinen Sitz in Köln habe, gab der HDBI im Januar 2018 die Überprüfung an die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW) ab. Nach acht Monaten verwies die LDI NRW aufgrund fehlender Zuständigkeit an den HDBI zurück. Eine Antwort von staatlicher Seite steht seitdem weiter aus.

Das hat sich der Gesetzgeber sicher anders vorgestellt, als er die Artikel 51 ff. DSGVO verabschiedet hat.

»*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.*« (Artikel 51 Absatz 2)

Zum Abschluss meiner Aufsichtstätigkeit nahm ich im Dezember 2018 an einem Gespräch von Vertretern der staatlichen Datenschutzaufsichten mit den Datenschutzbeauftragten der Kirchen und Medienanstalten teil, das an ein Erstgespräch im September 2017 anschloss.

Die staatlichen Aufsichtsbehörden hatten in einem Beschluss der DSK vom 06. Juni 2018 festgelegt, nach welchen Kriterien die Beteiligung der spezifischen Aufsichtsbehörden gemäß § 18 Absatz 1 Satz 4 BDSG-neu an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU zu erfolgen habe.

»*Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.* « (§ 18 Abs. 1 Satz 4 BDSG)

Problematisch ist, dass die DSGVO den Begriff der *»spezifischen Aufsichtsbehörde«* nicht kennt. Entsprechend kennt die DSGVO auch nur eine *»betroffene Aufsichtsbehörde«*. Die durch Bundesrecht und den DSK-Beschluss geschaffene *»über die allgemeine Mitbetroffenheit hinausgehende spezifische Betroffenheit einer Aufsichtsbehörde«* ist für mich als Landesaufsicht mangels Gesetzgebungskompetenz des Bundes nicht bindend. Ebensowenig Bindungswirkung entfaltet meines Erachtens die von der DSK ohne Teilnahme der Rundfunkdatenschutzbeauftragten getroffene Einschätzung, es liege *»eine Betroffenheit vor, wenn spezifische Fragen der Verarbeitung personenbezogener Daten durch die der Aufsicht der spezifischen Aufsichtsbehörden unterliegenden Stellen betroffen sind: bei der Erarbeitung von Stellungnahmen und der Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren i. S. v. Art. 70 DSGVO.*« (Ziffer 3b) des Beschlusses)

Der Dissens zwischen den Vertretern der DSK und den teilnehmenden Rundfunkdatenschutzbeauftragten konnte im Verlauf des Gesprächs nicht aufgelöst werden.

Man verständigte sich darauf, praktikable Lösungen für eine Beteiligung zu finden. Es wurde in Aussicht gestellt, dass die Rundfunkdatenschutzbeauftragten, in Abhängigkeit von Themen mit EU-Relevanz an Sitzungen der DSK-Arbeitskreise teilnehmen können. Die Bundesdatenschutzbeauftragte, bzw. ihr Nachfolger

wird den direkten Austausch mit den Rundfunkdatenschutzbeauftragten verstetigen. Angedacht ist insoweit ein Gedankenaustausch zweimal pro Jahr beziehungsweise anlassbezogen die Übersendung schriftlicher Informationen.

Zusammengefasst besteht also noch viel Raum für die Verbesserung der Zusammenarbeit der Aufsichtsbehörden, wie sie die DSGVO vorsieht.

7. Medienprivileg – ein großes Wort

Im journalistischen Bereich des WDR bin ich aufgrund des Medienprivilegs nur in Bezug auf die Einhaltung ausreichender technisch-organisatorischer Datensicherungsmaßnahmen aufsichtsbefugt.

Datenverarbeitung zu journalistischen Zwecken

Hintergrund des Medienprivilegs ist allgemein die Sicherung der in Artikel 5 Absatz 1 Satz 2 GG gewährleisteten Presse- und Rundfunkfreiheit gegenüber dem Staat. Das Medienprivileg folgt aus einer Abwägung zwischen dem Interesse einer Person am Schutz ihrer personenbezogenen Daten und der Bedeutung der Rundfunkfreiheit für ein pluralistisches Gemeinwesen.

Das Medienprivileg war bislang für den WDR in § 49 WDR-Gesetz alte Fassung geregelt. Auch die DSGVO sieht durch ihre Öffnungsklausel in Artikel 85 Absatz 1 und 2 weiter das Bedürfnis eines Ausgleichs zwischen dem *»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«.*

7.1. Rundfunkstaatsvertrag

Die Landesgesetzgeber haben diesen Ausgleich einheitlich durch die §§ 9c und 57 der Rundfunkstaatsverträge geschaffen:

»Für die Datenverarbeitung zu journalistischen Zwecken finden von der Verordnung 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.«

Neben allgemeinen Bestimmungen, Regeln zu Rechtsbehelfen, Haftung und Sanktionen, finden damit weiterhin vornehmlich die Vorschriften über geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung Anwendung.

Die Paragrafen des Rundfunkstaatsvertrags zum Medienprivileg sehen vor, dass sämtliche journalistisch tätigen Mitarbeiterinnen und Mitarbeiter auf das Datengeheimnis verpflichtet werden. Eine Verpflichtung auf das Datengeheimnis findet sich im Anhang (10.5).

Nach Erwägungsgrund 153 Satz 7 DSGVO *»müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden, um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen.«*

Kern der Privilegierung ist damit auch nach der DSGVO, dass das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt bei Datenverarbeitung zu journalistischen Zwecken nicht greift. Gäbe es diese Ausnahme nicht, wäre eine Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, eine Rechtsvorschrift erlaubte sie oder es läge eine diesbezügliche Einwilligung des Betroffenen vor. Könnten Journalistinnen und Journalisten personenbezogene Daten nur dann verarbeiten, wenn ein Gesetz dies gestattet oder die Betroffenen einwilligen, wäre die journalistische Tätigkeit massiv eingeschränkt. Freier und kritischer Journalismus als Kernelement der Rundfunkfreiheit und damit auch der demokratischen Grundordnung, wäre faktisch nicht möglich.

7.2. Betroffenen-Rechte

So sind auch die Betroffenen-Rechte in § 9c Absatz 3 Rundfunkstaatsvertrag spezialgesetzlich normiert:

»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.«

Die Betroffenenrechte sind in diesem Zusammenhang also zugunsten des Medienprivilegs stark eingeschränkt. Betroffene werden aber nicht schutzlos gestellt. Ihre Rechte leiten sich jedoch nicht aus Datenschutzrecht, sondern zum Beispiel aus dem allgemeinen Persönlichkeitsrecht im Rahmen von § 823 Absatz 1 BGB oder den §§ 22, 23 Kunsturhebergesetz (KUG) ab.

Betroffenen, die sich an mich wenden, um eine Veröffentlichung ihrer personenbezogenen Daten in der Berichterstattung des WDR zu verhindern, kann ich nicht helfen. Es handelt sich um eine Programmbeschwerde, keine Datenschutzbeschwerde.

Im Zuge der Neuerungen durch die DSGVO kam es zu Irritationen, ob die Anwendung dieser nationalen Gesetze im journalistischen Bereich von der DSGVO verdrängt werde. Das Oberlandesgericht Köln hat am 18. Juni 2018 in einem Verfügungsverfahren entschieden[13], dass das KUG im journalistischen Bereich weiterhin anwendbar ist.

7.3. Exkurs: Auskunftsersuchen

Ein Auskunftsrecht im Rahmen des Medienprivilegs steht dem Betroffenen demnach nur in sehr engen Grenzen zu.

Anfragen nach DSGVO müssen innerhalb eines Monats beantwortet werden. Bei besonders komplexen Anfragen oder einer besonders hohen Anzahl von Auskunftsersuchen, kann die Frist um zwei Monate verlängert werden. Anfragen können an die zentrale Funktions-E-Mail-Adresse Datenauskunft@wdr.de gerichtet werden, die zu diesem Zweck im Internet veröffentlicht wurde. Bei Auskunftsersuchen per Mail ist die Identifizierbarkeit ein Thema. Auskünfte zu im Zusammenhang mit E-Mail-Adressen gespeicherten personenbezogenen Daten, können nur an diese E-Mail-Adresse geschickt werden.

Das Angebot des WDR erfolgt weitestgehend nicht personalisiert und ohne Anmeldeerfordernisse. Aus datenschutzrechtlichen Gründen verfügt der WDR über keine zentrale Datenerfassung. In der Regel beziehen sich zulässige Auskunftsersuche deshalb auf den Zentralen Beitragsservice. Einen ersten Vorgeschmack darauf, was die Landesrundfunkanstalten und den Zentralen Beitragsservice ab dem 25. Mai 2018 erwarten könnte, gab es Mitte Mai als prominente Beitragsverweigerer Aufrufe zur Einreichung von Auskunftsersuchen im Netz verbreiteten, um die DSGVO dazu zu nutzen, den öffentlich-rechtlichen Rundfunk lahm zu legen.

Problematisch erschien insofern die Tatsache, dass Auskunftsersuchen laut Artikel 15 DSGVO keiner Präzisierung bedürfen, auf welche Information oder welche Verarbeitungsvorgänge sich das Auskunftsersuchen einer betroffenen Person bezieht. Allein Erwägungsgrund 63 Satz 7 erlaubt es, eine Präzision zu verlangen, wenn der Verantwortliche eine große Menge von Informationen über die betroffene Person verarbeitet. Erst am 16. Mai 2018 stellten CDU und FDP insofern einen Änderungsantrag in Bezug auf das Nordrhein-Westfälische Datenschutz-Anpassungs- und Umsetzungsgesetz EU, wonach der Satz *»Das Auskunftsrecht setzt voraus, dass die betreffende Person Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglicht.«* in das neue Datenschutzgesetz NRW übernommen wurde.

Der befürchtete Ansturm auf den WDR blieb aus. Beim Zentralen Beitragsservice sah das Bild in Bezug auf datenschutzrechtliche Eingaben aus NRW dagegen anders aus. Nachdem sich diese Vorgänge bis zum 24. Mai 2018 für das Jahr 2018 auf knapp 90 beschränkten, waren es ab dem 25. Mai 2018 knapp 1 190 datenschutzrechtliche Vorgänge aus dem Sendegebiet des WDR.

[13] OLG Köln, Beschluss vom 18.6.2018 – Aktenzeichen 15 W 27/18.

8. Stiftung Warentest, Apps und Tracking

In der Ausgabe Juli 2018 veröffentlichte die Stiftung Warentest unter der Rubrik Multimedia einen Test.

TV-Mediatheken: Apps von Fernsehsendern schicken Daten weiter

»Apps sind oft neugierig

Tendenziell sendeten die Smartphone-Apps der öffentlich-rechtlichen Sender weniger Daten als die der privaten und teilten sie mit weniger Partnerfirmen. Doch unkritisch fanden unsere Tester nur die Apps von SWR, WDR sowie die iOS-App des Bayrischen Rundfunks. «

Dieses Ergebnis schmeichelt dem WDR. Es zeigt aber auch die Gefahren, die eine technisch fehlerhafte App-Realisierung birgt.

Im Mai 2018 wurde ich von der Stiftung angeschrieben. Die Stiftung Warentest beschäftige sich in einer aktuellen Untersuchung mit dem Thema „Schutz von Nutzerdaten bei HbbTV Anwendungen (Mediatheken)“, insbesondere mit Datenschutz und Verarbeitung von Daten rund um das Smart TV. In diese Untersuchung werde auch *»die App des WDR«* einbezogen. Um Fehler zu vermeiden, bat Stiftung Warentest, die Versionsnummer auf Aktualität zu überprüfen und innerhalb einer Woche zu bestätigen.

Ich teilte der Stiftung Warentest mit, dass der WDR keine App im genannten Zusammenhang betreibe. Da mir Stiftung Warentest keine näheren Informationen darüber geben konnnte, welche App geprüft worden sei, schlossen wir aufgrund der angegebenen Versionierung auf die App „WDR – Hören, Sehen, Mitmachen“. Ich wies Stiftung Warentest darauf hin, dass es sich bei der App vorranging um eine Verbreitungs-App der Hörfunk- und Fernseh-Streams des WDR handelt. Innerhalb der App werde zwar per Link auf die WDR Mediathek im Web verwiesen, diese WDR App sei aber nicht als HBBTV- oder SmartTV-App nutzbar.

Generell wird bei der Umsetzung von Apps auf Datensparsamkeit geachtet. Erhobene Daten werden benötigt, um den zuverlässigen Betrieb der App sicherzustellen. In der Datenschutzerklärung muss hierüber informiert werden.

In der Android-App: „WDR – Hören, Sehen, Mitmachen“ fand kein Tracking innerhalb der nativen App statt. Gleiches galt für die iOS-Version. Bei Videoabrufen wurde zur Qualitätssicherung eine Software eingesetzt, die keine personenbezogenen oder personenbeziehbaren Daten verarbeitet.

8.1. Tracking und DSGVO

Aber was ist dieses Tracking und wie funktioniert das? Beim sogenannten Tracking handelt es sich um die Erhebung von Nutzungsinformationen. Um derartige Nutzungsinformationen zu erhalten müssen Nutzer wiedererkannt werden.

Im Web-Bereich werden hierfür in der Regel sogenannte Cookies verwandt. Cookies sind Textdateien, die der Web-Browser des Nutzers vom Web-Server des Diensteanbieters abruft und dann auf der Festplatte des Endgeräts speichert. Das auf dem Nutzerendgerät gespeicherte Cookie, kann vom Nutzer jederzeit gelöscht werden. Außerdem ist es möglich ein sogenanntes Opt-Out zu wählen. Opt-Out bedeutet, dass ein Cookie des Trackingtools im Browser gesetzt wird, das verhindert, dass Daten des Nutzers erhoben werden.

Im Rahmen von Mobile Apps generiert die Betriebssoftware des mobilen Endgeräts eine eindeutige Werbe-ID. Mobile Apps, die der Nutzer auf seinem Endgerät installiert hat, senden diese Werbe-ID an den Server des jeweiligen Diensteanbieters zur Identifizierung des Endgeräts.

Der WDR nutzt ausschließlich Endgeräte-IDs ohne Personenbezug, die keine Identifizierung einer natürlichen Person erlauben. Die DSGVO regelt nach ihrem sachlichen Anwendungsbereich ausschließlich die Verarbeitung personenbezogener Daten. Das Speichern und Abrufen von Geräte-IDs ohne Personenbezug fällt damit nicht in den Anwendungsbereich der DSGVO.

Bisher gilt in Deutschland gemäß § 15 Absatz 3 TMG für die Verwendung von Cookies die sogenannte Opt-Out-Lösung. Es ist erlaubt, pseudonyme Nutzungsprofile zu erfassen, die nur anonyme und pseudonyme Daten enthalten, sodass die Identität der Nutzer hieraus nicht abgeleitet werden kann. Beim Aufruf der Webseite muss hierüber in der Datenschutzerklärung informiert und den Nutzern die Möglichkeit gegeben werden, der Erstellung von Nutzungsprofilen zu widersprechen.

8.2. ePrivacy-Verordnung

Eigentlich sollte die ePrivacy-Verordnung zeitgleich mit der DSGVO Inkrafttreten. Der Vorschlag der europäischen Kommission vom 10.01.2017 sollte die bestehende ePrivacy-Richtlinie (Datenschutzrichtlinie für elektronische Kommunikation)[14] ersetzen.

Die ePrivacy Verordnung *»VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES 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)«* wurde Anfang 2017 von der EU-Kommission als offizieller Entwurf vorgestellt.[15] Sie wird wie die DSGVO als Verordnung keiner weiteren Umsetzung in nationales Recht der Mitgliedsstaaten bedürfen. Die E-Privacy-Verordnung wird alle Regelungen, die auf Grundlage der E-Privacy-Richtlinie ergangen sind, verdrängen und die rechtlichen Rahmenbedingungen der Messung des Nutzerverhaltens neu regeln.

Im Oktober 2017 stimmte das Europäische Parlament den Beschlussempfehlungen des federführenden Innenausschlusses zu. Jedoch ist eine Einigung mit der Europäischen Kommission und dem Ministerrat noch nicht in Sicht. Im Berichtszeitraum galt deshalb gemäß Artikel 95 DSGVO die bisherige E-Privacy-Richtlinie mit dem darauf basierenden Telemediengesetz fort.

Für den WDR ist vor allem die zukünftige Regelung des Webtracking von Interesse, da auch der WDR zur Webanalyse und Reichweitenmessung Webtracking durchführt. Abzuwarten bleibt, ob das Webtracking zukünftig mit der E-Privacy-Verordnung noch strenger reglementiert wird und der Einsatz von Tracking-Mechanismen einer Zustimmung bedarf.

Nach Artikel 8 Absatz 1 des offiziellen Entwurfs a) wäre das Setzen von Cookies möglich, soweit es für die Durchführung des elektronischen Kommunikationsvorgangs nötig ist, nach Buchstabe b), sofern der Endnutzer seine Einwilligung gegeben hat, c) es für die Bereitstellung des vom Endnutzer gewünschten Dienstes oder d) es für die Messung des Webpublikums nötig ist.

Hinsichtlich des Setzens von Cookies zu Marktforschungszwecken oder für eine Personalisierung von Angeboten besteht damit für die Zukunft eine gewisse Unsicherheit, wie sich die Haltung der Verordnungsgeber hierzu verhält. Was die Verordnung also letztendlich im Einzelnen für den WDR bedeuten wird, bleibt zum jetzigen Zeitpunkt abzuwarten.

[14] https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_de.pdf; RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

[15] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

9. BGH in eigener Sache

Mit seinem Urteil vom 15. Oktober 2018[16] hat der Bundesgerichtshof die Frage beantwortet, *»ob eine Tätigkeit im öffentlichen Dienst (hier: Rundfunkdatenschutzbeauftragte und behördliche Datenschutzbeauftragte des WDR sowie Leiterin des Datenschutzreferats dieser Rundfunkanstalt) einer Zulassung als Syndikusrechtsanwalt entgegensteht«*.[17]

9.1. Unabhängig

Fraglich war ob ein Zulassungsversagungsgrund nach § 46a Absatz 1 Nummer 2, § 7 Nummer 8 BRAO vorlag. Nach § 7 Nummer 8 BRAO, welcher auch für die Zulassung von Syndikusanwälten anzuwenden ist, ist eine Zulassung zu versagen, sofern die antragstellende Person eine Tätigkeit ausübt, die mit dem Beruf des Rechtsanwalts, insbesondere seiner Stellung als unabhängiges Organ der Rechtspflege nicht vereinbar ist oder das Vertrauen in seine Unabhängigkeit gefährden kann.

Der BGH hat in dem Urteil festgestellt, dass kein greifbarer Anhaltspunkt dafür bestehe, *»dass die Art der Tätigkeit der Beigeladenen, insbesondere die von dem Anwaltsgerichtshof insoweit herangezogene Funktion als Rundfunkdatenschutzbeauftragte, geeignet wäre, das Vertrauen der Bevölkerung in die Unabhängigkeit der Syndikusrechtsanwältin zu erschüttern. Dies gilt erst recht angesichts des Umstands, dass der Rundfunkdatenschutzbeauftragte gemäß § 53 Abs. 1 Satz 2 WDR-Gesetz (§ 50 Abs. 1 WDR-Gesetz n.F.) in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen ist.«*[18]

»Soweit der Anwaltsgerichtshof in diesem Zusammenhang meint, die vorbezeichnete datenschutzrechtliche Aufsichtsfunktion sei - trotz ihrer Staatsferne - grundsätzlich nicht mit dem Bild des Rechtsanwalts als unabhängigem Berater des Rechtsuchenden in Einklang, vermag dies in mehrfacher Hinsicht nicht zu überzeugen. Der Anwaltsgerichtshof hat hierbei bereits im Ansatz nicht hinreichend bedacht, dass auch ein als Datenschutzbeauftragter für seinen Mandanten tätiger selbständiger Rechtsanwalt an die datenschutzrechtlichen Vorschriften gebunden ist, ohne dass hierdurch die fachliche Unabhängigkeit seiner Tätigkeit oder die Eigenständigkeit seiner rechtlichen Analyse beeinträchtigt würde (vgl. nur Senatsbeschluss vom 1. August 2017 - AnwZ (Brfg) 14/17, NJW 2017, 2835 Rn. 12). Die von ihm in Ausübung dieser Vorschriften wahrgenommene datenschutzrechtliche Aufsichtsfunktion steht schon deshalb nicht im Widerspruch zu der unabhängigen Beraterfunktion des Rechtsanwalts, weil der Mandant den Anwalt mit der Wahrnehmung dieser Aufsichtsfunktion beauftragt hat.[19] *«*

»Hieran ändert der Umstand nichts, dass Dritte gemäß § 11 WDR-Gesetz das Recht haben, sich unmittelbar an den Rundfunkdatenschutzbeauftragten zu wenden. Durch dieses Anrufungsrecht nach § 11 WDR-Gesetz wird der Datenschutz des WDR nicht etwa insoweit zu einer Rechtsangelegenheit (auch) des Anrufenden, sondern bleibt vielmehr eine solche des WDR. Etwas anderes ergibt sich auch nicht aus dem von der Klägerin angeführten Gesichtspunkt, wonach die Unabhängigkeit eines Syndikusrechtsanwalts, deren Schutz gerade auch § 46 Abs. 5 BRAO diene (vgl. BT-Drucks. 18/5201, S. 30; Senatsurteil vom 2. Juli 2018 - AnwZ (Brfg) 49/17, aaO Rn. 49 f.), in einer solchen Situation durch einen möglichen Konflikt zwischen den Interessen des WDR und den Interessen des Anrufenden gefährdet sein könnte.«[20]

»Die Klägerin lässt hierbei außer Betracht, dass der Gesetzgeber mögliche Interessenkonflikte, die im Rahmen der Ausübung des - der Objektivität verpflichteten - Amtes des Rundfunkdatenschutzbeauftragten auftreten können, durchaus gesehen und deshalb zum Schutz der Unabhängigkeit des Rundfunkdatenschutzbeauftragten besondere Vorschriften in das Gesetz aufgenommen hat. Danach ist der Rundfunkdatenschutzbeauftragte des WDR in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen (§ 53 Abs. 1 Satz 2 WDR-Gesetz a.F.; § 50 Abs. 1 WDR-Gesetz n.F.); vergleichbare Schutzvorschriften enthalten die Datenschutzvorschriften auch für den behördlichen Da-tenschutzbeauftragten (vgl. § 4f Abs. 3 BDSG a.F.; § 6 Abs. 3, 4 BDSG n.F.; Art. 38 Abs. 3 Datenschutz-Grundverordnung; § 32a Abs. 2 DSG NRW a.F.; § 31 Abs. 4 DSG NRW n.F.). Von daher gesehen ist insbesondere auch in dem von der Klägerin

[16] BGH, Urteil vom 15. Oktober 2018 - AnwZ (Brfg) 20/18 - AGH Hamm.
[17] BGH- AnwZ (Brfg) 20/18; Seite 2 Buchstabe c).
[18] BGH- AnwZ (Brfg) 20/18; Randnummer 57.
[19] BGH- AnwZ (Brfg) 20/18; Randnummer 58.
[20] A.a.O. Randnummer 94.

angeführten Fall des Anrufungsrechts nach § 11 WDR-Gesetz eine Gefährdung der Unabhängigkeit weder hinsichtlich des Rundfunkdatenschutzbeauftragten des WDR noch hinsichtlich eines Syndikusrechtsanwalts, der - wie die Beigeladene - dieses Amt im Rahmen seiner Tätigkeit für den WDR bekleidet, zu besorgen.«[21]

Meine Unabhängigkeit ist also gewahrt.

9.2. Nicht hoheitlich

Auch enthalt die BRAO keine gesetzliche Bestimmung, welche die Zulassung eines im öffentlichen Dienst tätigen Angestellten als Syndikusrechtsanwalt allgemein ausschließt.

»Bei dem WDR, für den die Beigeladene als Angestellte tätig ist, handelt es sich zwar um eine (Rundfunk-)Anstalt des öffentlichen Rechts (§ 1 Abs. 1 Satz 1 WDR-Gesetz). Nach den von dem Anwaltsgerichtshof auf der Grundlage der oben genannten Tätigkeitsbeschreibung und des diese ergänzenden Schreibens der Beigeladenen vom 15. November 2016 getroffenen zutreffenden Feststellungen ist die Beigeladene für ihren Arbeitgeber im Wesentlichen zum einen als Rundfunkdatenschutzbeauftragte des WDR nach § 53 WDR-Gesetz a.F. (§§ 49 ff. WDR-Gesetz n.F.) - und damit gemäß § 53 Abs. 2 Satz 3 WDR-Gesetz a.F. in Verbindung mit § 32a des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW a.F.; vgl. nunmehr hingegen § 49 Abs. 4 WDR-Gesetz n.F.) zugleich als behördliche Datenschutzbeauftragte des WDR - und zum anderen, ebenfalls auf dem Gebiet des Datenschutzrechts, in beratender, vertragsgestaltender und verhandlungsführender Funktion tätig.«[22]

»Die Tätigkeit der Beigeladenen für ihren aus den vorstehend genannten Gründen grundsätzlich nicht hoheitlich handelnden Arbeitgeber wird, wie der Anwaltsgerichtshof insoweit richtig erkannt hat, auch nicht etwa deshalb zu einer hoheitlichen Tätigkeit, weil die Beigeladene nach § 53 Abs. 1 Satz 1 WDR-Gesetz a.F. in ihrer Eigenschaft als Rundfunkdatenschutzbeauftragte an die Stelle des Landesbeauftragten für den Datenschutz tritt. Stellt die Beigeladene als Rundfunkdatenschutzbeauftragte einen Verstoß gegen datenschutzrechtliche Vorschriften fest, steht ihr das Mittel der Beanstandung gegenüber dem Intendanten - unter gleichzeitiger Unterrichtung des Rundfunkrats - zur Verfügung (§ 53 Abs. 3 bis 6 WDR-Gesetz a.F.; § 51 Abs. 2 bis 4 WDR-Gesetz n.F.). Hierin sieht auch die Klägerin - zu Recht - weder einen Verwaltungsakt noch sonst ein hoheitliches Handeln.«[23]

»Es kann jedoch dahinstehen, ob § 46 Abs. 5 BRAO, wie die Klägerin meint, voraussetzt, dass der Syndikusrechtsanwalt im Rahmen der Tätigkeit für seinen Arbeitgeber ausschließlich in dessen Rechtsangelegenheiten tätig ist und es nicht ausreicht, wenn das Arbeitsverhältnis durch Rechtsangelegenheiten des Arbeitgebers (§ 46 Abs. 2 Satz 1, Abs. 5 BRAO) geprägt ist. Denn die Beigeladene ist, auch soweit es um ihre Anrufung als Rundfunkdatenschutzbeauftragte (§ 11 WDR-Gesetz) geht, ausschließlich in Rechtsangelegenheiten ihres Arbeitgebers, des WDR, tätig. Dieser ist für seinen Bereich der Verantwortliche für den Datenschutz. Der Datenschutz ist daher seine Rechtsangelegenheit (vgl. auch Senatsurteil vom 2. Juli 2018 - AnwZ (Brfg) 49/17, aaO Rn. 44). Die Tätigkeit der Beigeladenen als Rundfunkdatenschutzbeauftragte des WDR dient - wie bereits die durch den Gesetzgeber formulierte amtliche Gesetzesüberschrift (vgl. hierzu BGH, Urteil vom 21. März 2018 - VIII ZR 104/17, NJW 2018, 2187 Rn. 37 mwN) sowohl des § 53 WDR-Gesetz a.F. als auch des § 49 WDR-Gesetz n.F. deutlich macht - der „Gewährleistung des Datenschutzes beim WDR“, indem sie die Einhaltung der Datenschutzvorschriften überwacht (§ 53 Abs. 2 Satz 1 WDR-Gesetz a.F.; § 51 Abs. 1 Satz 1 WDR-Gesetz n.F.). Damit ist die Beigeladene auch in ihrer Eigenschaft als Rundfunkdatenschutzbeauftragte des WDR in dessen Rechtsangelegenheiten tätig.«[24]

[21] A.a.O. Randnummer 95.
[22] A.a.O. Randnummer 51.
[23] A.a.O. Randnummer 54.
[24] A.a.O. Randnummer 93.

10. Anhang

10.1. Auszug aus EuGH, Urteil vom 05.06.2018 – C-210/16

[…]

24 Unter diesen Umständen hat das Bundesverwaltungsgericht beschlossen, das Verfahren auszusetzen und dem Gerichtshof die folgenden Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 2 Buchst. d der Richtlinie 95/46 dahin auszulegen, dass er Haftung und Verantwortlichkeit für Datenschutzverstöße abschließend und erschöpfend regelt, oder verbleibt im Rahmen der „geeigneten Maßnahmen“ nach Art. 24 dieser Richtlinie und der „wirksame[n] Einwirkungsbefugnisse“ nach Art. 28 Abs. 3 Spiegelstrich 2 dieser Richtlinie in mehrstufigen Informationsanbieterverhältnissen Raum für eine Verantwortlichkeit einer Stelle, die nicht im Sinne von Art. 2 Buchst. d dieser Richtlinie für die Datenverarbeitung verantwortlich ist, bei der Auswahl eines Betreibers für ihr Informationsangebot?

2. Folgt aus der Pflicht der Mitgliedstaaten nach Art. 17 Abs. 2 der Richtlinie 95/46, bei der Datenverarbeitung im Auftrag vorzuschreiben, dass der für die Verarbeitung Verantwortliche einen „Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichend Gewähr bietet“, im Umkehrschluss, dass bei anderen Nutzungsverhältnissen, die nicht mit einer Datenverarbeitung im Auftrag im Sinne von Art. 2 Buchst. e dieser Richtlinie verbunden sind, keine Pflicht zur sorgfältigen Auswahl besteht und auch nach nationalem Recht nicht begründet werden kann?

[…]

Zu den Vorlagefragen

Zur ersten und zur zweiten Frage

25 Mit der ersten und der zweiten Frage, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob Art. 2 Buchst. d, Art. 17 Abs. 2, Art. 24 und Art. 28 Abs. 3 zweiter Gedankenstrich der Richtlinie 95/46 dahin auszulegen sind, dass sie es zulassen, dass die Verantwortlichkeit einer Stelle in ihrer Eigenschaft als Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage im Fall eines Verstoßes gegen die Vorschriften über den Schutz personenbezogener Daten aufgrund der Entscheidung, ein soziales Netzwerk für die Verbreitung ihres Informationsangebots zu nutzen, festgestellt wird.

26 Zur Beantwortung dieser Fragen ist darauf hinzuweisen, dass die Richtlinie 95/46, wie sich aus ihrem Art. 1 Abs. 1 und ihrem zehnten Erwägungsgrund ergibt, darauf abzielt, ein hohes Niveau des Schutzes der Grundfreiheiten und Grundrechte natürlicher Personen, insbesondere ihrer Privatsphäre, bei der Verarbeitung personenbezogener Daten zu gewährleisten (Urteil vom 11. Dezember 2014, Ryneš, C‑212/13, EU:C:2014:2428, Rn. 27 und die dort angeführte Rechtsprechung).

27 Diesem Ziel entsprechend ist der Begriff des „für die Verarbeitung Verantwortlichen“ in Art. 2 Buchst. d der Richtlinie weit definiert als natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

28 Wie der Gerichtshof bereits entschieden hat, besteht das Ziel dieser Bestimmung nämlich darin, durch eine weite Definition des Begriffs des „Verantwortlichen“ einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten (Urteil vom 13. Mai 2014, Google Spain und Google, C‑131/12, EU:C:2014:317, Rn. 34).

29 Zudem verweist der Begriff des „für die Verarbeitung Verantwortlichen“, da er sich, wie Art. 2 Buchst. d der Richtlinie 95/46 ausdrücklich vorsieht, auf die Stelle bezieht, die „allein oder gemeinsam mit anderen“ über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, nicht zwingend auf eine einzige Stelle und kann mehrere an dieser Verarbeitung beteiligte Akteure betreffen, wobei dann jeder von ihnen den Datenschutzvorschriften unterliegt.

30 Es ist festzustellen, dass im vorliegenden Fall in erster Linie die Facebook Inc. und, was die Union betrifft, Facebook Ireland über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen entscheiden, die die auf Facebook unterhaltenen Fanpages besucht haben, und somit unter den Begriff des „für die Verarbeitung Verantwortlichen“ im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 fallen, was in der vorliegenden Rechtssache nicht in Zweifel gezogen wird.

31 Zur Beantwortung der vorgelegten Fragen ist jedoch zu prüfen, ob und inwieweit der Betreiber einer auf Facebook unterhaltenen Fanpage wie die Wirt-

schaftsakademie im Rahmen dieser Fanpage gemeinsam mit Facebook Ireland und der Facebook Inc. einen Beitrag zur Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher dieser Fanpage leistet und somit ebenfalls als „für die Verarbeitung Verantwortlicher" im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 angesehen werden kann.

32 Insoweit schließt offenbar jede Person, die eine Fanpage auf Facebook einrichten möchte, mit Facebook Ireland einen speziellen Vertrag über die Eröffnung einer solchen Seite und unterzeichnet dazu die Nutzungsbedingungen dieser Seite einschließlich der entsprechenden Cookie-Richtlinie, was zu prüfen Sache des nationalen Gerichts ist.

33 Wie aus den dem Gerichtshof vorgelegten Akten hervorgeht, erfolgt die im Ausgangsverfahren in Rede stehende Datenverarbeitung im Wesentlichen in der Weise, dass Facebook auf dem Computer oder jedem anderen Gerät der Personen, die die Fanpage besucht haben, Cookies platziert, die die Speicherung von Informationen in den Web-Browsern bezwecken und für die Dauer von zwei Jahren wirksam bleiben, sofern sie nicht gelöscht werden. Außerdem geht aus den Akten hervor, dass in der Praxis Facebook die in den Cookies gespeicherten Informationen empfängt, aufzeichnet und verarbeitet, insbesondere wenn eine Person die „Facebook-Dienste, Dienste, die von anderen Mitgliedern der Facebook-Unternehmensgruppe bereitgestellt werden, und Dienste, die von anderen Unternehmen bereitgestellt werden, die die Facebook-Dienste nutzen", besucht. Außerdem können andere Stellen wie Facebook-Partner oder sogar Dritte „auf den Facebook-Diensten Cookies verwenden, um [diesem sozialen Netzwerk direkt] bzw. den auf Facebook werbenden Unternehmen Dienstleistungen bereitzustellen".

34 Diese Verarbeitungen personenbezogener Daten sollen u. a. zum einen Facebook ermöglichen, sein System der Werbung, die es über sein Netzwerk verbreitet, zu verbessern. Zum anderen sollen sie dem Betreiber der Fanpage ermöglichen, zum Zweck der Steuerung der Vermarktung seiner Tätigkeit Statistiken, die Facebook aufgrund der Besuche dieser Seite erstellt, zu erhalten, die es ihm beispielsweise ermöglichen, Kenntnis von den Profilen der Besucher zu erlangen, die seine Fanpage schätzen oder die seine Anwendungen nutzen, um ihnen relevantere Inhalte bereitstellen und Funktionen entwickeln zu können, die für sie von größerem Interesse sein könnten.

35 Auch wenn der bloße Umstand der Nutzung eines sozialen Netzwerks wie Facebook für sich genommen einen Facebook-Nutzer nicht für die von diesem Netzwerk vorgenommene Verarbeitung personenbezogener Daten mitverantwortlich macht, ist indes darauf hinzuweisen, dass der Betreiber einer auf Facebook unterhaltenen Fanpage mit der Einrichtung einer solchen Seite Facebook die Möglichkeit gibt, auf dem Computer oder jedem anderen Gerät der Person, die seine Fanpage besucht hat, Cookies zu platzieren, unabhängig davon, ob diese Person über ein Facebook-Konto verfügt.

36 In diesem Rahmen geht aus den dem Gerichtshof unterbreiteten Angaben hervor, dass die Einrichtung einer Fanpage auf Facebook von Seiten ihres Betreibers eine Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten impliziert, die sich auf die Verarbeitung personenbezogener Daten zum Zweck der Erstellung der aufgrund der Besuche der Fanpage erstellten Statistiken auswirkt. Mit Hilfe von durch Facebook zur Verfügung gestellten Filtern kann der Betreiber die Kriterien festlegen, nach denen diese Statistiken erstellt werden sollen, und sogar die Kategorien von Personen bezeichnen, deren personenbezogene Daten von Facebook ausgewertet werden. Folglich trägt der Betreiber einer auf Facebook unterhaltenen Fanpage zur Verarbeitung der personenbezogenen Daten der Besucher seiner Seite bei.

37 Insbesondere kann der Fanpage-Betreiber demografische Daten über seine Zielgruppe – und damit die Verarbeitung dieser Daten – verlangen, so u. a. Tendenzen in den Bereichen Alter, Geschlecht, Beziehungsstatus und berufliche Situation, Informationen über den Lebensstil und die Interessen seiner Zielgruppe und Informationen über die Käufe und das Online-Kaufverhalten der Besucher seiner Seite, die Kategorien von Waren oder Dienstleistungen, die sie am meisten interessieren, sowie geografische Daten, die ihn darüber informieren, wo spezielle Werbeaktionen durchzuführen oder Veranstaltungen zu organisieren sind, und ihm ganz allgemein ermöglichen, sein Informationsangebot so zielgerichtet wie möglich zu gestalten.

38 Zwar werden die von Facebook erstellten Besucherstatistiken ausschließlich in anonymisierter Form an den Betreiber der Fanpage übermittelt, jedoch beruht die Erstellung dieser Statistiken auf der vorhergehenden Erhebung – durch die von Facebook auf dem Computer oder jedem anderen Gerät der Personen, die diese Seite besucht haben, gesetzten Cookies – und der Verarbeitung der personenbezogenen Daten dieser Besucher für diese statistischen Zwecke. Die Richtlinie 95/46 verlangt jedenfalls nicht, dass bei einer gemeinsamen Verantwortlichkeit mehrerer Betreiber für dieselbe Verarbeitung jeder Zugang zu den betreffenden personenbezogenen Daten hat.

39 Unter diesen Umständen ist festzustellen, dass der Betreiber einer auf Facebook unterhaltenen Fanpage wie die Wirtschaftsakademie durch die von ihm vorgenommene Parametrierung u. a. entsprechend

seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt ist. Daher ist der Betreiber im vorliegenden Fall als in der Union gemeinsam mit Facebook Ireland für diese Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 einzustufen.

40 Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.

41 Im Übrigen ist hervorzuheben, dass die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst.

42 Unter diesen Umständen trägt die Anerkennung einer gemeinsamen Verantwortlichkeit des Betreibers des sozialen Netzwerks und des Betreibers einer bei diesem Netzwerk unterhaltenen Fanpage im Zusammenhang mit der Verarbeitung personenbezogener Daten der Besucher dieser Fanpage dazu bei, entsprechend den Anforderungen der Richtlinie 95/46 einen umfassenderen Schutz der Rechte sicherzustellen, über die die Personen verfügen, die eine Fanpage besuchen.

43 Klarzustellen ist, dass das Bestehen einer gemeinsamen Verantwortlichkeit, wie der Generalanwalt in den Nrn. 75 und 76 seiner Schlussanträge ausgeführt hat, aber nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat, die von einer Verarbeitung personenbezogener Daten betroffen sind. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.

44 Nach alledem ist auf die erste und die zweite Frage zu antworten, dass Art. 2 Buchst. d der Richtlinie 95/46 dahin auszulegen ist, dass der Begriff des „für die Verarbeitung Verantwortlichen“ im Sinne dieser Bestimmung den Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage umfasst.

[…]

10.2. Seiten-Insights-Ergänzung bezüglich des Verantwortlichen

Facebook stellt dir für deine Seite Seiten-Insights zur Verfügung. Bei Seiten-Insights handelt es sich um zusammengefasste Daten, durch die du Aufschluss darüber erlangen kannst, wie die Menschen mit deiner Seite interagieren. Um mehr über die dir in Verbindung mit deiner Seite zur Verfügung stehenden Seiten-Insights zu erfahren, nutze bitte den Insights-Tab auf deiner Seite.

Seiten-Insights können auf personenbezogenen Daten basieren, die im Zusammenhang mit einem Besuch oder einer Interaktion von Personen auf bzw. mit deiner Seite und ihren Inhalten erfasst wurden. Wenn du in der Europäischen Union/im Europäischen Wirtschaftsraum wohnst und sofern diese personenbezogenen Daten unter deinem Einfluss und deiner Kontrolle (bzw. dem-/derjenigen irgendeines Dritten, für den du die Seite erstellst oder verwaltest) im Rahmen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „DSGVO“) verarbeitet werden, („Insights-Daten“), erkennst du in deinem eigenen Namen (und als Vertreter für jedweden sonstigen Dritt-Verantwortlichen, für den du die Seite erstellst oder verwaltest, und in dessen Namen) an und stimmst zu, dass diese Seiten-Insights-Ergänzung bezüglich des Verantwortlichen („Seiten-Insights-Ergänzung“) gilt:

Facebook Ireland Limited („Facebook Ireland“) und du seid gemeinsam Verantwortliche für die Verarbeitung von Insights-Daten. Diese Seiten-Insights-Ergänzung legt die jeweiligen Verantwortlichkeiten von Facebook Ireland und dir im Hinblick auf die Verarbeitung von Insights-Daten fest.

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.

Du solltest sicherstellen, dass du eine Rechtsgrundlage für die Verarbeitung von Insights-Daten gemäß DSGVO hast, den Verantwortlichen für die Verarbeitung der Seite benennst und jedwede sonstigen geltenden rechtlichen Pflichten erfüllst.

Du stimmst zu, dass nur Facebook Ireland Entscheidungen hinsichtlich der Verarbeitung von Insights-Daten treffen und umsetzen kann. Facebook Ireland entscheidet nach seinem alleinigen Ermessen, wie es seine Pflichten gemäß dieser Seiten-Insights-Ergänzung erfüllt. Du stimmst zu, dass Facebook Ireland in der EU die Hauptniederlassung für die Verarbeitung von Insights-Daten für sämtliche Verantwortliche ist. Außerdem erkennst du an, dass die irische Datenschutzkommission die federführende Aufsichtsbehörde für diese Verarbeitung ist.

Facebook Ireland bleibt alleinig verantwortlich für die Verarbeitung solcher personenbezogenen Daten im Zusammenhang mit Seiten-Insights, die nicht unter diese Seiten-Insights-Ergänzung fallen. Diese Seiten-Insights-Ergänzung gewährt dir kein Recht, die Offenlegung von im Zusammenhang mit Facebook-Produkten verarbeiteten personenbezogenen Daten von Facebook-Nutzern zu verlangen, einschließlich für Seiten-Insights, welche wir dir bereitstellen.

Wenn eine betroffene Person oder eine Aufsichtsbehörde gemäß DSGVO hinsichtlich der Verarbeitung von Insights-Daten und der von Facebook Ireland im Rahmen dieser Seiten-Insights-Ergänzung übernommenen Pflichten Kontakt mit dir aufnimmt (jeweils eine „Anfrage"), bist du verpflichtet, uns unverzüglich, jedoch spätestens innerhalb von 7 Kalendertagen sämtliche relevanten Informationen weiterzuleiten. Zu diesem Zweck kannst du dieses Formular einreichen. Facebook Ireland wird Anfragen im Einklang mit den uns gemäß dieser Seiten-Insights-Ergänzung obliegenden Pflichten beantworten. Du stimmst zu, zeitnah sämtliche angemessenen Anstrengungen zu unternehmen, um mit uns an der Beantwortung jedweder derartigen Anfrage zusammenzuarbeiten. Du bist nicht berechtigt, im Namen von Facebook Ireland zu handeln oder zu antworten.

Wenn du eine Seite für irgendeinen geschäftlichen oder gewerblichen Zweck nutzt bzw. auf sie zugreifst (u. a. wenn du eine Seite für ein Unternehmen verwaltest), stimmst du zu, dass jedweder Anspruch, Klagegenstand oder Streitfall, den du uns gegenüber hast und der sich aus dieser Seiten-Insights-Ergänzung ergibt oder damit in Verbindung steht, ausschließlich von den Gerichten in Irland zu klären ist, dass du dich für das Prozessieren jedwedes derartigen Anspruchs unwiderruflich der Rechtsprechung der irischen Gerichte unterwirfst und dass diese Seiten-Insights-Ergänzung irischem Recht unterliegt.

Möglicherweise müssen wir diese Seiten-Insights-Ergänzung von Zeit zu Zeit aktualisieren. Deshalb empfehlen wir dir, sie regelmäßig auf Aktualisierungen zu prüfen. Durch deinen weiteren Zugriff auf Seiten bzw. deren weitere Nutzung nach irgendeiner Benachrichtigung über eine Aktualisierung dieser Seiten-Insights-Ergänzung stimmst du zu, an sie gebunden zu sein. Solltest du der aktualisierten Seiten-Insights-Ergänzung nicht zustimmen, beende bitte jedwede Nutzung von Seiten. Wenn du ein Verbraucher mit ständigem Wohnsitz in einem Mitgliedstaat der Europäischen Union bist, gilt nur 4.1 unserer Facebook-Nutzungsbedingungen für Aktualisierungen dieser Seiten-Insights-Ergänzung.

Sollte irgendein Teil dieser Seiten-Insights-Ergänzung für nicht durchsetzbar erachtet werden, so bleiben die übrigen Bestimmungen in vollem Umfang wirksam und in Kraft. Ein Versäumnis unsererseits, irgendeinen Teil dieser Seiten-Insights-Ergänzung durchzusetzen, stellt keinen Rechtsverzicht dar. Jedwede Änderung dieser Nutzungsbedingungen oder der Verzicht auf diese muss in schriftlicher Form erfolgen und von uns unterzeichnet werden.

„personenbezogene Daten", „betroffene Person" und „Verantwortlicher" haben in dieser Seiten-Insights-Ergänzung die ihnen in der DSGVO zugewiesenen Bedeutungen.

10.3. Stellungnahme des AK DSB zur möglichen Einführung von Office 365 in der Europa-Cloud

Management Summary

Derzeit gibt es in mehreren öffentlich-rechtlichen Rundfunkanstalten Überlegungen zur Einführung von Office 365 in der Europa-Cloud-Variante. Der AK DSB wurde mit Blick auf diese Entwicklung gebeten zu prüfen, ob es datenschutzrechtlich möglich ist, Office 365 in der Variante der Europa- Cloud in den Rundfunkanstalten einzuführen.

Aus Sicht des AK DSB würde mit einem solchen Umstieg ein Paradigmenwechsel begangen. Es würde im großen Umfang die Verarbeitung von Unternehmensdaten und personenbezogenen Daten in die Hände eines Dritten und in die Cloud gegeben. Dies ist mit datenschutzrechtlichen Risiken verbunden. Aufgrund der Tragweite des damit verbundenen Systemwechsels und der entsprechenden Risiken handelt es sich dabei aus Sicht der Datenschutzbeauftragten um eine Managemententscheidung, bei der die datenschutzrechtlichen Risiken unbedingt berücksichtigt werden müssen.

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten sehen insbesondere folgende datenschutzrechtliche Risiken:

\ Mit der Einführung der Europa-Cloud besteht ein erhöhtes Risiko des Zugriffs Dritter auf die Daten der Sender. Dieses resultiert daraus, dass zum einen auch bei einer Europa-Cloud keine strenge Lokalisierung der Daten auf europäische Server stattfindet, sondern auch hier Daten außerhalb des europäischen Rechtsraumes verarbeitet werden. Zum anderen werden die Daten durch ein US-amerikanisches Unternehmen mit Hauptsitz in den USA verarbeitet. Damit einher geht eine gesteigerte Möglichkeit des Zugriffs auf unsere Daten durch ausländische und US-amerikanische Behörden, wie Geheimdienste und Strafverfolgungsbehörden (Stichwort: Prism u. a.). Diese Risiken sind aus Sicht des Datenschutzes insbesondere relevant für die Verarbeitung von investigativen journalistischen Informationen, aber auch für sensible personenbezogene Daten von Mitarbeitern und Dritten. Der Schutz der sensiblen journalistischen Recherchedaten ist Kernaufgabe des öffentlich-rechtlichen Rundfunks. Er ist elementarer Bestandteil und gleichzeitig Voraussetzung der Rundfunkfreiheit und darf durch die Einführung von Office 365 in der Cloud nicht gefährdet werden.

\ Datenschutzrechtlich relevant ist darüber hinaus, dass die Kontrolle über die Datenverarbeitung in einem solchen Modell in großem Umfang in die Hände eines Dritten gelegt wird. Auch hierin besteht ein Systemwechsel. Wie letztendlich genau die Datenverarbeitung durch Microsoft erfolgt, ist nur schwer nachzuhalten. Hier sind die Sender weitgehend angewiesen auf Informationen, die von Microsoft über Internetseiten zur Verfügung gestellt werden, die kontinuierlich angepasst werden, auf mündliche Aussagen bzw. auf Testate und Zertifizierungen. Letztendlich verlangt das Modell daher auch, dass man dem Vertragspartner nach der gebotenen sorgfältigen Prüfung vertraut. Ein großes Stück der Kontrolle gibt man in diesem Modell ab.

\ Außerdem besteht ein datenschutzrechtliches Risiko in der Datenverarbeitung außerhalb von Europa, die auch in der Europa-Cloud-Variante stattfindet. Auch hier wird nur für einen Teil der Daten (die „ruhenden Daten“) eine Speicherung in Europa garantiert. Dies birgt insofern ein Problem, als die Datenverarbeitung außerhalb von Europa nur unter bestimmen rechtlichen Voraussetzungen zulässig ist. Die hier derzeit zur Verfügung stehenden Rechtsinstrumente (Stichwort: Privacy Shield, Standardvertragsklauseln) sind jedoch datenschutzrechtlich umstritten. Es besteht die Gefahr, dass sie gerichtlich aufgehoben werden. In diesem Fall würde die Rechtsgrundlage für eine Verarbeitung von personenbezogenen Daten außerhalb des EWR entfallen. Die Daten müssten zurückgeholt werden.

\ Außerdem ist das Risiko der Verfügbarkeit der Daten zu betrachten. Mit Einführung von Office 365 in der Europa-Cloud werden wesentliche Funktionalitäten wie z. B. E-Mail in die Cloud ausgelagert. Bei einem Zusammenbruch der Leitungsverbindung stünden sie nicht mehr zur Verfügung.

Aufgrund dieser Risiken sollte vor der Entscheidung für eine Europa-Cloud-Variante geprüft werden, ob – wenn die Sender zu dem Ergebnis kommen, dass eine Auslagerung der Datenverarbeitung unverzichtbar ist – auch ein Betrieb von Office 365 in Deutschland im besten Fall mit Ausschluss eines Datentransfers in die USA (z. B. in der sog. Private Cloud der Telekom) für die Rundfunkanstalten ein gangbarer Weg sein kann.

Sollten die Rundfunkanstalten nach Abwägung aller Vorteile und Risiken dennoch zu dem Ergebnis kommen, Office 365 mit der Europa-Cloud einführen zu wollen, so ist dies nur unter folgenden datenschutzrechtlichen Voraussetzungen möglich:

1. Microsoft muss tatsächlich und vertraglich die Einhaltung der erforderlichen technischen Sicherheitsmaßnahmen garantieren, um die Sicherheit der Daten zu gewährleisten. Dies ist durch entsprechende Testate (z. B. C 5 Zertifizierung nach BSI) nachzuweisen. Insoweit wird auch auf die Prüfungen der IT-Sicherheitsbeauftragten verwiesen.

2. Auch bei Office 365 ist zu gewährleisten, dass hoch vertrauliche personenbezogene Daten, insbesondere vertrauliche investigative Recherchedaten nicht in der Cloud verarbeitet werden und die Möglichkeit der lokalen Speicherung auch weiterhin technisch gewährleistet wird. Dies setzt voraus, dass in den Häusern eine entsprechende Informationsklassifizierung vorgenommen wird und eine Festlegung erfolgt, wie mit vertraulichen Daten umzugehen ist.

3. Es ist ein Auftragsdatenverarbeitungsvertrag (unter der DS-GVO Auftragsverarbeitungsvertrag) abzuschließen, der den Vorgaben der DS-GVO entspricht und die datenschutzrechtlichen Verantwortlichkeiten sowie die Kontrollrechte der Sender regelt.

4. Neben dem Auftragsdatenverarbeitungsvertrag sind zusätzlich die von der Europäischen Kommission genehmigten Standardvertragsklauseln abzuschließen.

5. Für den Fall, dass die derzeit bestehenden rechtlichen Instrumentarien, die eine Datenverarbeitung außerhalb des europäischen Rechtsraums ermöglichen, für unzulässig erklärt werden, ist die Rückholbarkeit der Daten zu gewährleisten.

Rahmenbedingungen der Prüfung des AK DSB

Basis der datenschutzrechtlichen Bewertung waren die von Microsoft zur Verfügung gestellten Unterlagen, die von den Anstalten übermittelten Informationen zu den Plänen der Sender sowie Informationen aus den Gesprächen mit Microsoft. Dabei ist darauf hinzuweisen, dass die von den Anstalten selbst übermittelten Anforderungen bis zuletzt insoweit lückenhaft waren, als die Bedarfe der Anstalten nur unkonkret formuliert wurden. Insbesondere erfolgte keine Konkretisierung der Kategorien bzw. der Arten personenbezogener Daten, die verarbeitet werden sollen. Auch ein Schutzbedarf für die in der Anwendung bzw. Cloud zu verarbeitenden Daten wurde nicht festgelegt. Da die sicherheitstechnischen und datenschutzrechtlichen Anforderungen jedoch stets abhängig sind vom Schutzbedarf der zu verarbeitenden Daten ist eine wesentliche Voraussetzung für eine abschließende Beurteilung bis heute nicht erfüllt.

Die vorliegende Stellungnahme enthält daher neben der Darstellung der rechtlichen Rahmenbedingungen auch Vorgaben zur Umsetzung, die nach Auffassung der Datenschutzbeauftragten von ARD, ZDF und DR bei der Einführung von Office 365 in der Cloud gegeben sein müssen.

Die Datenschutzbeauftragten weisen ausdrücklich darauf hin, dass sich ihre datenschutzrechtliche Bewertung ausschließlich auf die in Diskussion befindliche Cloud-Nutzung bezieht. Sie beinhaltet keine Prüfung und Bewertung der einzelnen Office 365-Anwendungen/-Module und deren spezifischen Datenverarbeitung. Sollten sich die Sender für eine Einführung von Office 365 entscheiden, ist für die jeweils einzelnen Module und die darin stattfindende konkrete Datenverarbeitung eine separate Bewertung erforderlich, die auch ein IT-Sicherheitskonzept für die konkret geplante Cloud-Nutzung umfassen muss.

Datenschutzrechtliche Bewertung der Verarbeitung von personenbezogenen Daten in der Europa-Cloud von Microsoft im Rahmen von Office 365

1. Grundlagen der datenschutzrechtlichen Bewertungen

Basis einer datenschutzrechtlichen Bewertung der Cloud-Nutzung ist der grundsätzliche Umgang mit personenbezogenen Daten in der Cloud. Dieser soll im Folgenden zunächst dargestellt und sodann rechtlich eingeordnet werden.

2. Allgemeines und Umgang mit personenbezogenen Daten

a.) Vertragliche Situation

Bei einer Wahl der Europa-Cloud schließt die Rundfunkanstalt die vertraglichen Vereinbarungen ausschließlich mit Microsoft. Nach aktueller Rechts- und Vertragslage wird ein Grundvertrag einschließlich Auftragsdatenverarbeitungsvertrag zwischen dem Sender und Microsoft Irland geschlossen. Parallel dazu erfolgt der Abschluss von Standardvertragsklauseln zwischen dem Sender und Microsoft USA.

b.) Ort der Datenverarbeitung

Nach den dem AK DSB vorliegenden Informationen erfolgt eine Verarbeitung von personenbezogenen Daten bei der Nutzung der sog. Europa-Cloud innerhalb und außerhalb von Europa, d. h. europäischen Rechenzentren. Eine vollständige Beschränkung der Verarbeitung auf europäische Rechenzentren sagt Microsoft lediglich für die sog. „ruhenden Daten“ zu. Was darunter zu verstehen ist, wird in den dem AK DSB vorliegenden Unterlagen vertraglich nicht eindeutig definiert. Es ist jedoch davon auszugehen, dass von dem Begriff all diejenigen Daten erfasst werden, die sich nicht in Bearbeitung oder im Transport befinden. Nach dem derzeitigen Kenntnisstand ist davon auszugehen, dass sowohl die personenbezogenen Daten des Active Directory, als auch personenbezogene Daten im Supportfall und Daten im Transfer (Daten, die beim Zugriff auf die Cloudanwendungen vom Arbeitsplatz zur Cloud, bzw. umgekehrt transportiert werden) nicht ausschließlich in Europa, sondern zumindest auch in den USA verarbeitet werden. Korrekt wäre daher nicht von Europa-Cloud zu sprechen, sondern vielmehr von einer Global-Cloud, mit der präferierten Lokalisierung eines Teils der Daten in der Europäischen Union.

3. Datenschutzrechtliche Bewertung

a.) Erforderlichkeit des Abschlusses eines Auftragsdatenverarbeitungsvertrages

Die datenschutzrechtliche Bewertung der Einführung von Office 365 in der Europa-Cloud muss anhand der Regelungen der DS-GVO erfolgen, die ab Mai 2018 Gültigkeit erlangt, da eine Einführung nach diesem Zeitpunkt ins Auge gefasst wird. Grundsätzlich ist es auch unter der DS-GVO möglich im entsprechenden Umfang personenbezogene Daten durch einen Dienstleister wie im Falle von Office 365 verarbeiten zu lassen, wenn ein entsprechender Auftragsdatenverarbeitungsvertrag (Art. 28 DS-GVO) abgeschlossen wird. Dieser regelt die Verantwortlichkeiten zwischen den beiden Parteien beim Umgang mit personenbezogenen Daten. Er legt u. a. fest, dass der Auftragnehmer – hier Microsoft als Auftragsverarbeiter– die Daten ausschließlich im Auftrag der Rundfunkanstalten verarbeiten darf. Microsoft ist zum Abschluss eines solchen Vertrages verpflichtet und bereit. Die Datenschutzbeauftragten gehen aufgrund der bislang geführten Gespräche und den gesichteten Unterlagen davon aus, dass es im Rahmen

der konkreten Vertragsverhandlungen gelingen wird, hier datenschutzkonforme Verträge abzuschließen. Abschließend beurteilt werden kann dies jedoch erst bei Vorlage der Vertragsentwürfe.

b.) Grundsatz der Verarbeitung von personenbezogenen Daten innerhalb des Europäischen Wirtschaftsraumes

Die DS-GVO enthält wie auch die bislang geltenden datenschutzrechtlichen Regelungen den Grundsatz, dass personenbezogene Daten grundsätzlich nur im Geltungsbereich des Europäischen Datenschutzrechts verarbeitet werden. Eine Verarbeitung von personenbezogenen Daten außerhalb dieses Geltungsbereichs ist nur in Ausnahmefällen möglich, wenn gewährleistet wird, dass bei der Verarbeitung auch außerhalb des EWR-Raumes ein vergleichbares Datenschutzniveau besteht.

c.) Voraussetzungen für eine Datenverarbeitung außerhalb des EWRs nach der DS-GVO

Ein angemessenes Datenschutzniveau kann auf unterschiedliche Art und Weise gewährleistet werden, nämlich wenn

\ die EU-Kommission die Angemessenheit in dem „Empfangsland“ durch Beschluss festgestellt hat (Angemessenheitsbeschluss der EU-Kommission, z. B. Privacy Shield für Datentransfer in die USA; Art. 45 DS-GVO);

\ geeignete Garantien vorliegen dafür, dass die Rechte der Betroffenen nicht eingeschränkt werden (z. B. Vereinbarung von Standardvertragsklauseln; Art. 46 DS-GVO)

\ Ausnahmen für bestimmte Fälle gegeben sind (Art. 49 DS-GVO).

d.) Herangehensweise von Microsoft bei Office 365 in der Europa-Cloud zur Absicherung des Datentransfers in die USA

Microsoft versucht diesen datenschutzrechtlichen Anforderungen auf zwei Wegen gerecht zu werden: Zum einen haben sie sich den Regelungen des Privacy Shield unterworfen und zum anderen schließen sie mit ihren Kunden neben einem Auftragsdatenverarbeitungsvertrag die von der Europäischen Kommission genehmigten Standardvertragsklauseln ab.

e.) Rechtliche Problematik des Privacy Shield

Die EU-Kommission hat für das US-Privacy Shield in einem Angemessenheitsbeschluss (zukünftig Art. 45 DS-GVO) festgestellt, dass bei einer Datenverarbeitung durch US-Firmen in den USA ein angemessenes Datenschutzniveau gegeben ist, wenn sie sich den Regelungen des Privacy Shield unterworfen haben. Allerdings ist das Privacy Shield aus Datenschutzsicht hoch umstritten und wird auch bereits gerichtlich angefochten. Ob es der gerichtlichen Überprüfung standhält, ist stark zu bezweifeln. Zwar schafft es gegenüber dem vom EuGH gekippten Safe Harbor-Abkommen verbesserte Datenschutzbedingungen. Es ist allerdings äußerst fraglich, ob diese ausreichend sind. Vor diesem Hintergrund ist von einem umfangreichen und dauerhaft geplanten Datentransfer in die USA wie im Rahmen von Office 365 geplant ausschließlich auf Basis des Privacy Shields unbedingt abzuraten.

f.) Rechtliche Problematik der Standardvertragsklauseln

Aber auch eine Rechtfertigung des Datentransfers in die USA auf Basis von sog. Standardvertragsklauseln birgt datenschutzrechtliche Risiken. In 2001 hat die EU-Kommission durch Beschluss festgestellt, dass unter Verwendung der Standardvertragsklauseln eine Datenverarbeitung außerhalb des EWR-Raums grundsätzlich stattfinden kann. Die vertraglichen Regelungen, so der Schluss der EU-Kommission, bieten ausreichende Garantien für einen datenschutzkonformen Umgang mit personenbezogenen Daten. Dabei regeln die Vertragsparteien in den Standardvertragsklauseln u. a. ihre jeweiligen Verpflichtungen zur Einhaltung des Datenschutzes zum Umgang mit Beschwerden von Betroffenen zur Information über Anfragen Dritter einschließlich Behörden und zur Kontrolle durch die Aufsichtsbehörden.

Mit Blick auf die Entwicklungen in den USA, insbesondere den Erkenntnissen zum Vorgehen der Geheimdienste und nicht zuletzt auch im Hinblick auf das Vorgehen der Regierung von Donald Trump werden auch die Standardvertragsklauseln zunehmend hinterfragt. Auch hier findet derzeit eine gerichtliche Überprüfung vor den Gerichten in Irland statt (Max Schrems, der Kläger des Safe Harbor-Verfahrens, hatte die Irische Datenschutzaufsichtsbehörde wegen der Datenverarbeitung durch Facebook in den USA angerufen. Daraufhin hat die Datenschutzaufsichtsbehörde Facebook vor den ordentlichen Gerichten verklagt mit der Argumentation, die Verwendung von Standardvertragsklauseln garantiere keinen angemessenen Datenschutz). Im Zuge dieses Verfahrens wird auch der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsverfahrens angerufen werden. Die Vorlagefragen werden gegenwärtig formuliert. Die Standardvertragsklauseln bieten damit zwar gegenwärtig eine rechtliche Basis zur Datenverarbeitung außerhalb des EWR. Der Fortbestand dieses Rechtsinstruments ist jedoch nicht garantiert.

g.) Vertraulichkeit der Daten und Zugriff durch US-Behörden

Jenseits dieser rechtlichen, die Rechtsgrundlage des Datentransfers betreffenden Risiken, besteht außerdem das Risiko, dass die Daten bei Microsoft nicht vertraulich behandelt werden. Insbesondere zu betrachten ist hier der Zugriff durch Dritte, insbesondere auch US-amerikanische Behörden. Zum einen steht hier die sicherlich schwer zu beurteilende Möglichkeit des Datenzugriffs durch US-Geheimdienste im Raum. Zum anderen ist bis heute nicht abschließend gerichtlich geklärt, ob nach US-amerikanischem Recht in Europa gespeicherte Daten vor einer Herausgabe an US-amerikanische Strafverfolgungsbehörden wirksam geschützt sind. Derzeit ist beim US-Supreme Court ein Verfahren anhängig in dem zu entscheiden ist, ob Microsoft E-Mail-Korrespondenz, die auf seinen Servern in der EU gespeichert ist, aufgrund eines Beschlagnahmebeschlusses an die Strafverfolgungsbehörden herausgeben muss. Nachdem Microsoft das Berufungsverfahren für sich und gegen eine Herausgabe entscheiden konnte, ist der Ausgang der Revision derzeit noch offen.

h.) Eingeschränkte Kontrollmöglichkeiten

Schlussendlich geht die Einführung von Office 365 in der Europa-Cloud mit einer grundsätzlichen Einschränkung der Kontrollmöglichkeiten einher. Unabhängig von dem datenschutzrechtlich erforderlichen und vertraglich zu vereinbarenden Kontrollrechts, sind die Möglichkeiten der Kontrolle beschränkt auf die Informationen, die Microsoft seinen Kunden zur Verfügung stellt und solchen die in Testaten oder Zertifikaten ggfs. auch von Dritten bescheinigt werden. Dabei haben die bisherigen Gespräche mit Microsoft gezeigt, wie schwierig es ist jenseits von Verweisen auf wechselnde Informationen auf Internetplattformen verbindliche Aussagen von Microsoft zu konkreten Datenverarbeitungsprozessen zu bekommen.

Besondere Vorgaben für die Verarbeitung von personenbezogenen Daten in der Cloud aus Sicht der Datenschutzbeauftragten von ARD und ZDF

Sollten sich die Rundfunkanstalten entscheiden, Office 365 in der Variante der Europa-Cloud einzuführen, so ist dies aus Sicht der Datenschutzbeauftragten angesichts der oben beschriebenen Rechtslage und der bestehenden Risiken nur unter den folgenden Voraussetzungen möglich:

1. Keine hochvertraulichen Daten insbesondere zu investigativen Recherchen in der Cloud

Die o. g. Ausführungen haben die datenschutzrechtlichen Risiken aufgezeigt. Vor diesem Hintergrund sollte aus Sicht der Datenschutzbeauftragten von einer Verarbeitung von hoch vertraulichen, bzw. sensiblen personenbezogenen Daten in der Cloud abgesehen werden. Dies gilt neben sensiblen Mitarbeiterdaten insbesondere auch für besonders schützenswerte Informationen und personenbezogene Daten aus investigativen Recherchen. Eine Speicherung dieser Daten außerhalb des europäischen Datenschutzrechtsraumes ist aus Sicht der Datenschutzbeauftragten nicht vertretbar. Der Schutz der sensiblen journalistischen Recherchedaten ist Kernaufgabe des öffentlich-rechtlichen Rundfunks. Er ist elementarer Bestandteil und gleichzeitig Voraussetzung der Rundfunkfreiheit. Auch bei Einführung von Office 365 in der Cloud-Variante ist zu gewährleisten, dass eine On-Premise-Verarbeitung solch sensibler und besonders schützenswerter Daten auch weiterhin gewährleistet wird.

2. IT-Sicherheitsanforderungen

Nach der DS-GVO (insbesondere Art. 5, Abs. 1 f) und Art. 32 DS-GVO) sind personenbezogene Daten so zu verarbeiten, dass eine angemessene Sicherheit gewährleistet wird. Es ist die Integrität und Vertraulichkeit der Daten sicherzustellen, d. h. insbesondere auch der Schutz vor dem unbefugten Zugriff und/oder Manipulation durch Dritte zu gewährleisten. Dazu ist es erforderlich, dass Sicherheitsmaßnahmen umgesetzt und vertraglich auch zugesichert werden, die dem Stand der Technik und den Schutzbedarf der Daten entsprechen. Insoweit wird auf die Prüfung der AG ITS verwiesen.

3. Rückholbarkeit der Daten

Aufgrund der dargestellten datenschutzrechtlichen Risiken betreffend die Rechtsgrundlage einer Datenverarbeitung außerhalb des EWR ist auf eine Rückholbarkeit der Daten zu achten. Bei Ausgestaltung der Verträge ist zudem eine Regelung aufzunehmen, die eine Anpassung an geänderte rechtliche Voraussetzung ermöglicht.

4. ADV-Vertrag und Standardvertragsklauseln

Wie beschrieben muss ein Auftragsdatenverarbeitungsvertrag von Standardvertragsklauseln abgeschlossen werden, die den Anforderungen der DS-GVO entsprechen. Nach Prüfung der bislang von Microsoft vorgelegten Unterlagen und den geführten Gesprächen gehen die Vertreter des AK DSB davon aus, dass durch den Abschluss eines entsprechenden Auftragsdatenverarbeitungsvertrages und die Vereinbarung von Standardvertragsklauseln datenschutzkonforme Verträge abgeschlossen werden können. Eine detaillierte Prüfung und abschließende Bewertung kann allerdings erst mit Vorlage der tatsächlichen Vertragsentwürfe vorgenommen werden.

10.4. Muster-Vereinbarung Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

.....
- nachstehend Auftraggeber genannt -
(oder auch Verantwortlicher genannt) und dem/der

.....

- nachstehend Auftragsverarbeiter (oder auch Auftragnehmer) genannt -

.....

zur Verarbeitung personenbezogener Daten* im Auftrag nach Art. 28 DSGVO

*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, Art. 4 Ziff. 1 DSGVO

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand:

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung, Leistungsbeschreibung vom…… auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder ☐ Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter:
……(Definition der Aufgaben)

(2) Dauer:

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht) Der Auftrag wird zur einmaligen Ausführung erteilt.

oder ☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

§ 2 Konkretisierung des Auftragsinhalts

(1) Art der Daten:

☐ Die Art der zu verarbeitenden personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder ☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

☐ Personaldaten

☐ Kommunikationsdaten (z.B. Telefon, E-Mail)

☐ Log-Dateien

☐ IP-Adressen

☐ personenbezogene Planungs- und Steuerungsdaten

☐ personenbezogene Vertragsdaten

☐ personenbezogene Abrechnungs- und Zahlungsdaten

☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) .....

(2) Betroffener Personen:

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder ☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Zuschauer/Zuhörer

☐ Nutzer Online-Angebote

☐ Beschäftigte

☐ Geschäftspartner

☐ Ansprechpartner

☐ Beitragszahler/potentielle Beitragszahler

☐ .....

(3) Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten:

☐ Der Zweck der Verarbeitung personenbezogener Daten durch den Auftrag für den Auftraggeber ist konkret beschrieben in der Leistungsvereinbarung vom…… oder ☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf den Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter:

……

(4) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in

……

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DSGVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO);

☐ wird hergestellt durch sonstige Maßnahmen: ……(Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DSGVO)

§ 3 Verantwortlichkeit

(1) Die Auftragsverarbeitung richtet sich nach Artikel 28 DSGVO. Der Auftraggeber ist als Verantwortlicher für die Einhaltung der anzuwendenden Datenschutzvorschriften im Hinblick auf die Verarbeitung seiner Daten verantwortlich. Er hat insbesondere zu prüfen, ob die Datenverarbeitung zulässig ist.

(2) Macht eine betroffene Person datenschutzrechtliche Ansprüche (z.B. auf Auskunft) geltend, so unterstützt der Auftragsverarbeiter den Auftraggeber bei der Erfüllung dieser Pflichten. Der Auftragsverarbeiter trifft für diese Unterstützung technische und organisatorische Maßnahmen nach dem Stand der Technik. Welche Tätigkeiten der Auftragsverarbeiter im Rahmen der Unterstützung auszuführen hat, bestimmt sich im jeweiligen Einzelfall.

(3) Der Auftraggeber hat als Verantwortlicher die Pflichten aus Art. 32 – 36 DSGVO zu erfüllen. Der Auftragsverarbeiter unterstützt ihn bei der Erfüllung dieser Pflichten und zwar auch gegenüber den Aufsichtsbehörden. Der Auftragsverarbeiter trifft auch für diese Unterstützung die erforderlichen technischen und organisatorischen Maßnahmen nach dem Stand der Technik.

§ 4 Weisungsbefugnis

(1) Der Auftragsverarbeiter darf die Daten nur im Rahmen dieses Auftrags und nach den Weisungen des Auftraggebers verarbeiten. Eine Verarbeitung für andere Zwecke – worunter insbesondere eigene Zwecke des Auftragsverarbeiters fallen – ist nicht zulässig.

(2) Der Auftraggeber entscheidet allein und ausschließlich über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten.

(3) Weisungen können generell oder im Einzelfall erteilt werden. Sie sind schriftlich zu erteilen, was auch in elektronischer Form erfolgen kann. Für mündlich erteilte Weisungen ist unverzüglich die Schriftform nachzuholen.

(4) Der Auftragsverarbeiter hat den Auftraggeber zu unterrichten, wenn eine Weisung nicht unverzüglich durchgeführt werden kann. Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, so informiert er unverzüglich den Verantwortlichen.

§ 5 Technisch-organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragsverarbeiter ist verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung zu überwachen. Er versichert, dass er die Regelungen der Art. 25 und Art. 32 DSGVO einhält, beachtet und dokumentiert. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen. Die verwendeten Daten werden von sonstigen Datenbeständen getrennt.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen und ein entsprechendes Sicherheitskonzept vorzulegen. Die zu treffenden Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten siehe Anlage).

☐ Der Auftragsverarbeiter hat sich hierzu wie folgt zertifizieren lassen (Nennung der Zertifikate mit Nennung und Gültigkeitsdauer):
……

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 6 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragsverarbeiter sicherzustellen.

(3) Wird festgestellt, dass Daten unrichtig sind, hat der Auftragsverarbeiter den Auftraggeber hierüber zu informieren und nach dessen Weisung unverzüglich zu berichtigen. Daten, für welche die Voraussetzungen des Art. 18 DSGVO vorliegen, dürfen nur entsprechend eingeschränkt verarbeitet werden.

(4) Anfallendes Test- und Ausschussmaterial wird vom Auftragsverarbeiter unter Verschluss gehalten, bis es entweder vom Auftragsverarbeiter datenschutzgerecht gelöscht bzw. vernichtet oder dem Auftraggeber übergeben wird. Löschungen sind mit Protokollen zu dokumentieren und dem Auftraggeber auf Verlangen zur Verfügung zu stellen. Es muss eine rückinformationssichere Vernichtung gemäß DIN 66399 gewährleistet sein, ein Transport in verschlossenen Behältern vorgenommen werden und eine protokollierte und dokumentierte physische Vernichtung erfolgen (siehe auch unter § 14 dieses Vertrages).

§ 7 Vertraulichkeit

(1) Der Auftragsverarbeiter verpflichtet sich, die ihm vom Auftraggeber zur Verfügung gestellten Unterlagen und Daten sowie die Arbeitsergebnisse vertraulich zu behandeln, insbesondere Unbefugten nicht zugänglich zu machen und dem Auftraggeber hierzu jederzeit Auskunft zu geben.

(2) Der Auftragsverarbeiter gewährleistet die Einhaltung der Vertraulichkeit. Er sichert zu, alle für ihn im Rahmen der Ausführung dieses Auftrags tätigen Personen auf die Vertraulichkeit zu verpflichten. Soweit Personen einer gesetzlichen Verschwiegenheitspflicht in Bezug auf diese Tätigkeit unterliegen und deshalb eine Verpflichtung auf Vertraulichkeit nicht erfolgen soll, ist der Verzicht auf die Vereinbarung auf die Vertraulichkeit nur zulässig, wenn diese gesetzliche Verschwiegenheitspflicht einen angemessenen Schutz bietet.

(3) Bei einer Kontrolle durch Stellen, die einem Informationsfreiheitsgesetz unterliegen, ist dafür Sorge zu tragen, dass Betriebs- und Geschäftsgeheimnisse des Auftraggebers gewahrt und wirtschaftliche Informationen geschützt werden.

(4) Diese Verpflichtungen bestehen auch nach Beendigung des Vertrages fort.

§ 8 Sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragsverarbeiter Herr/Frau ……

[Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

oder ☐ Der Auftragsverarbeiter ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner für Fragen zu Datenschutz und Informationssicherheit im Zusammenhang mit diesem Vertrag wird beim Auftragsverarbeiter Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

☐ Da der Auftragsverarbeiter seinen Sitz außerhalb der Union hat, benennt er folgenden, auch schon im Rubrum dieses Vertrages benannten Vertreter nach Art. 27 Abs. 1 DSGVO in der Union:

[Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im

Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

§ 9 Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen (Art. 28 Abs. 2 DSGVO).

a) ☐ Eine Unterbeauftragung ist unzulässig.

oder b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden

Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO:

Firma Unterauftragnehmer Anschrift/Land
Leistung

oder c) ☐ Die Auslagerung auf Unterauftragnehmer

☐ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

\ der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

\ der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

\ eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(2) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(3) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von

Abs. 1 Satz 2 eingesetzt werden sollen. Auf § 2 Abs. 4 wird insoweit verwiesen.

(4) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet; oder

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(5) Der Auftragsverarbeiter wird auf Verlangen dem Auftraggeber Kopien der Unteraufträge zur Verfügung stellen und alle erforderlichen Auskünfte erteilen.

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Es wird Bezug genommen auf § 5 dieses Vertrages.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

☐ Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision,

Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Der Auftragsverarbeiter unterwirft sich auch der Kontrolle durch die für den Auftraggeber zuständige Aufsichtsbehörde, soweit Daten des Auftraggebers betroffen sind.

§ 11 Haftung

(1) Der Auftragsverarbeiter haftet für die ordnungsgemäße Ausführung des Auftrags nach den gesetzlichen Bestimmungen, insbesondere nach Art. 82 Abs. 2 EU-DSGVO. Machen betroffene Personen Ansprüche gegenüber dem Verantwortlichen wegen unzulässiger oder unrichtiger Datenverarbeitung geltend, so hat der Auftragsverarbeiter den Verantwortlichen zu unterstützen und zu beweisen, dass die fehlerhafte Datenverarbeitung nicht in seinem eigenen Verantwortungsbereich liegt.

(2) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

(3) Der Auftragsverarbeiter haftet für Verschulden eines weiteren Auftragsverarbeiters bzw. Subunternehmers wie für eigenes Verschulden.

§ 12 Informationspflichten des Auftragverarbeiters

(1) Der Auftragsverarbeiter wird den Auftraggeber darauf hinweisen, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Bis zur Bestätigung der Weisung durch den Auftraggeber ist der Auftragsverarbeiter nicht verpflichtet, die Weisung auszuführen.

(2) Bei schwerwiegenden Störungen des Betriebsablaufs oder bei Verdacht auf Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) oder wesentlichen Unregelmäßigkeiten bei der Datenverarbeitung unterrichtet der Auftragsverarbeiter gemäß Art. 33 II DSGVO unverzüglich den Auftraggeber. Dasselbe gilt, wenn sich eine Aufsichtsbehörde oder Strafverfolgungsorgane bei dem Auftragsverarbeiter melden.

(3) Sollen die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden oder droht eine wesentliche Änderung der Eigentumsverhältnisse beim Auftragsverarbeiter, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang involvierten Personen unverzüglich darüber informieren, dass die Hoheit der Daten beim Auftraggeber liegt.

§ 13 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts an Daten und Unterlagen ist während der Vertragsdauer und danach (gleichgültig aus welchem Grund das Auftragsverhältnis endet) ausgeschlossen.

§ 14 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 15 Sonstiges

(1) Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile -einschließlich etwaiger Zusicherung des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrages handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.

(2) Die Unwirksamkeit einer Bestimmung dieses Vertrages berührt nicht die Gültigkeit der übrigen Bestimmungen. Die Parteien werden unwirksame Bestimmungen durch wirtschaftlich ihnen nahekommende neue Bestimmungen ersetzen.

(Ort), den……Ort), den ……

(Auftraggeber) (Auftragsverarbeiter)

Anlage – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

\ Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

\ Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

\ Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

\ Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing, Trennung von Produktiv-, Test- und Entwicklungsumgebungen;

\ Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

\ Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Speicherung, Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

\ Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert, kopiert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

\ Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), Redundanz- und/oder Havarie-Konzepte, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

\ rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

\ Rückholbarkeit sämtlicher Daten.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

\ Datenschutz-Management;

\ Incident-Response-Management;

\ datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

\ Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

10.5. Datengeheimnis

10.5.1. Verpflichtung §§ 9c, 57 RStV

Soweit ich bei meiner Tätigkeit personenbezogene Daten zu journalistischen Zwecken verarbeite, ist es mir untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Ich bin mir darüber im Klaren, dass das Datengeheimnis auch nach Beendigung meiner Tätigkeit fortbesteht.

Für die Datenverarbeitung zu journalistischen Zwecken müssen personenbezogene Daten 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“).

Mir ist bekannt, dass Verstöße gegen das Datengeheimnis gemäß §§ 33, 34 DSG NRW geahndet werden können. Das Merkblatt zur Verpflichtung auf das Datengeheimnis habe ich erhalten.

10.5.2. Merkblatt

Aus dem Rundfunkstaatsvertrag NRW (RStV)

§ 9 c Datenverarbeitung zu journalistischen Zwecken, Medienprivileg [§ 57]

(1) Soweit die in der ARD zusammengeschlossenen Landesrundfunkanstalten (…) [als Anbieter von Telemedien] personenbezogene Daten zu journalistischen Zwecken verarbeiten, 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. (…)

Aus der Datenschutzgrundverordnung (DSGVO)

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen:

(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“);

Aus dem Landesdatenschutzgesetz (DSG NRW)

§ 33 DSG NRW – Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, entgegen den Vorschriften über den Datenschutz in diesem Gesetz oder in anderen Rechtsvorschriften des Landes Nordrhein-Westfalen personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,

2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht. Der Versuch ist strafbar. (…)

§ 34 DSG NRW – Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften über den Datenschutz in diesem Gesetz oder in anderen Rechtsvorschriften des Landes Nordrhein-Westfalen personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,

2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst.

Ordnungswidrig handelt auch, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 100.000 Deutschen Mark oder 50.000 Euro geahndet werden. (…)

IMPRESSUM

Herausgeber
Westdeutscher Rundfunk Köln
Anstalt des öffentlichen Rechts
Marketing
Appellhofplatz 1
50667 Köln

Redaktion
Datenschutzbeauftragte Karin Wagner
Leiterin Datenschutzreferat

März 2019

WESTDEUTSCHER
RUNDFUNK

Appellhofplatz 1
50667 Köln

wdr.de